MODELOS DE SEGURIDAD EN WEB

Modelos de seguridad en Web

Objetivos:

- Conocer las distintos modelos prácticos de seguridad en Internet
- Estudiar los túneles de cifrado a través de Internet
- Describir los servicios de seguridad ofrecidos por el nivel SSL (Secure Sockets Layer) para su aplicación en el acceso a Bases de Datos
- Servicios de Seguridad a nivel de Aplicación (correo S/MIME, Comercio Electrónico etc)

Modelos de seguridad en Web
Nivel de seguridad SSL

Índice:

- Modelos de seguridad en Internet
- Túneles de cifrado en Internet (IPSEC/IPV6)
- Servicios de seguridad SSL
  - Protocolo de transporte SSL (Record Protocol)
  - Protocolo de Autenticación SSL (Handshake Protocol
  - Protocolos adicionales SSL
- Aplicaciones seguras: Correo seguro S/MIME Comercio electrónico SET

MODELOS DE SEGURIDAD EN INTERNET

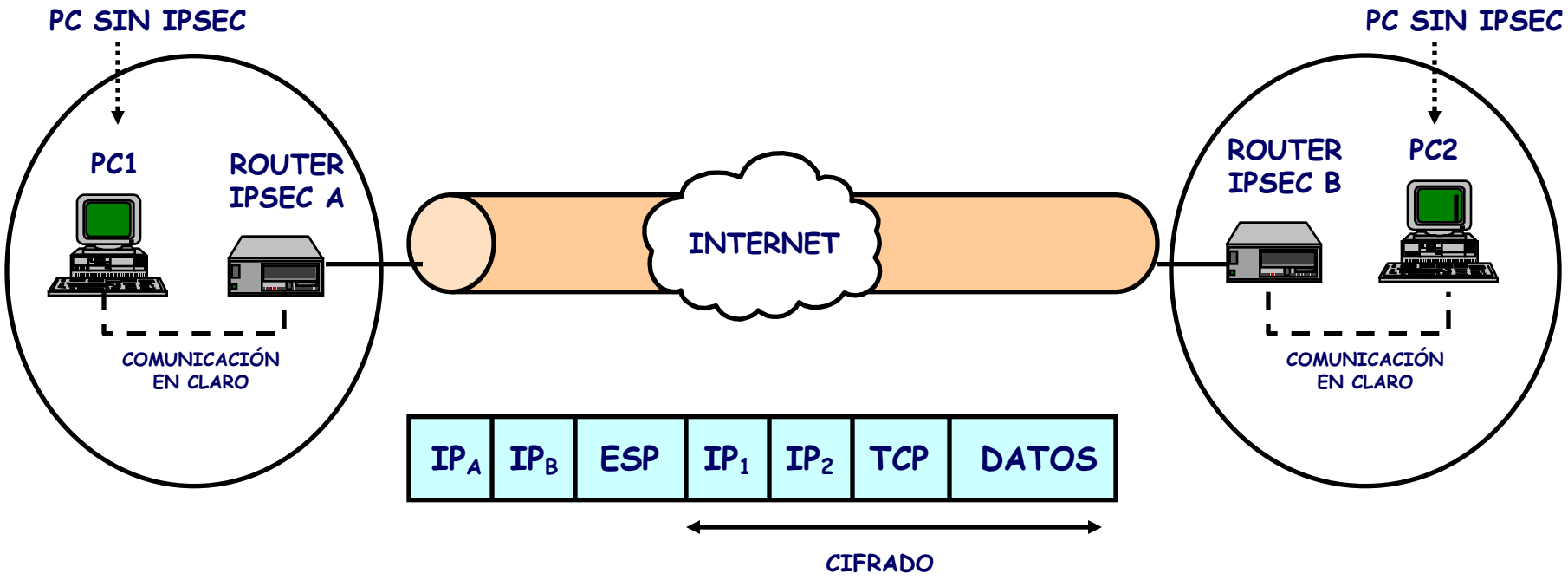
- Seguridad en el nivel de Red
  - IPSec /IPv6
- Seguridad en el nivel de transporte
  - Una capa adicional de seguridad transparente a los niveles superiores
- Seguridad a nivel de aplicación
  - Orientado a aplicaciones específicas

COMPONENTES DE IPSEC

- Una Arquitectura (RFC 2401)
  - RFCs 1826, 1827, 2401, 2402, 2406 y 2408
- Servicios:
  - AUTENTICACIÓN (AH, Authentication header). RFC 2402
  - CONFIDENCIALIDAD (ESP, Encapsulation Security Payload). RFC 2406
- Mecanismo de Gestión de Seguridad Basado en Asociaciones de Seguridad
  - SPI (Security Parameters Index)
- Mecanismo De Intercambio Dinámico De Claves
  - IKE: Internet Key Interchange. RFC 2408

IPSEC:

TÚNEL DE CIFRADO A TRAVÉS DE LA INTERNET

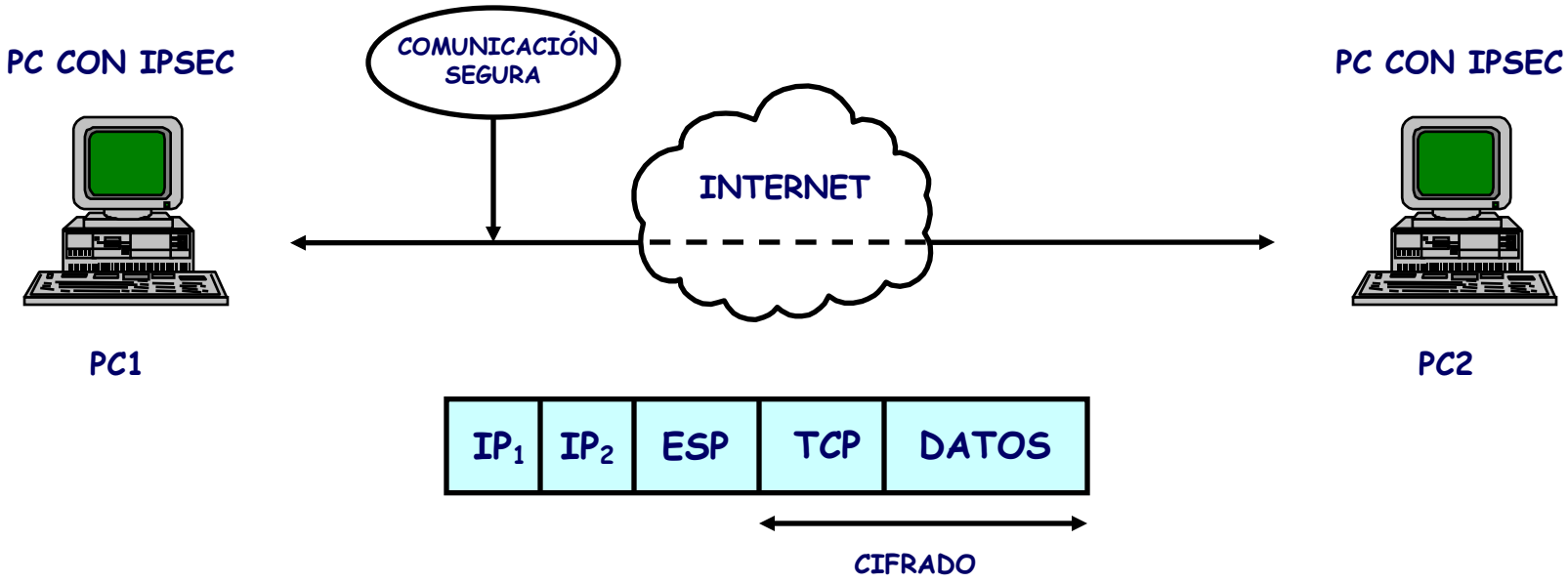


PAQUETE IPSEC MODO TÚNEL

ESP: Encapsulation Security Payload

IPSEC:

CONFIDENCIALIDAD MODO TRANSPORTE

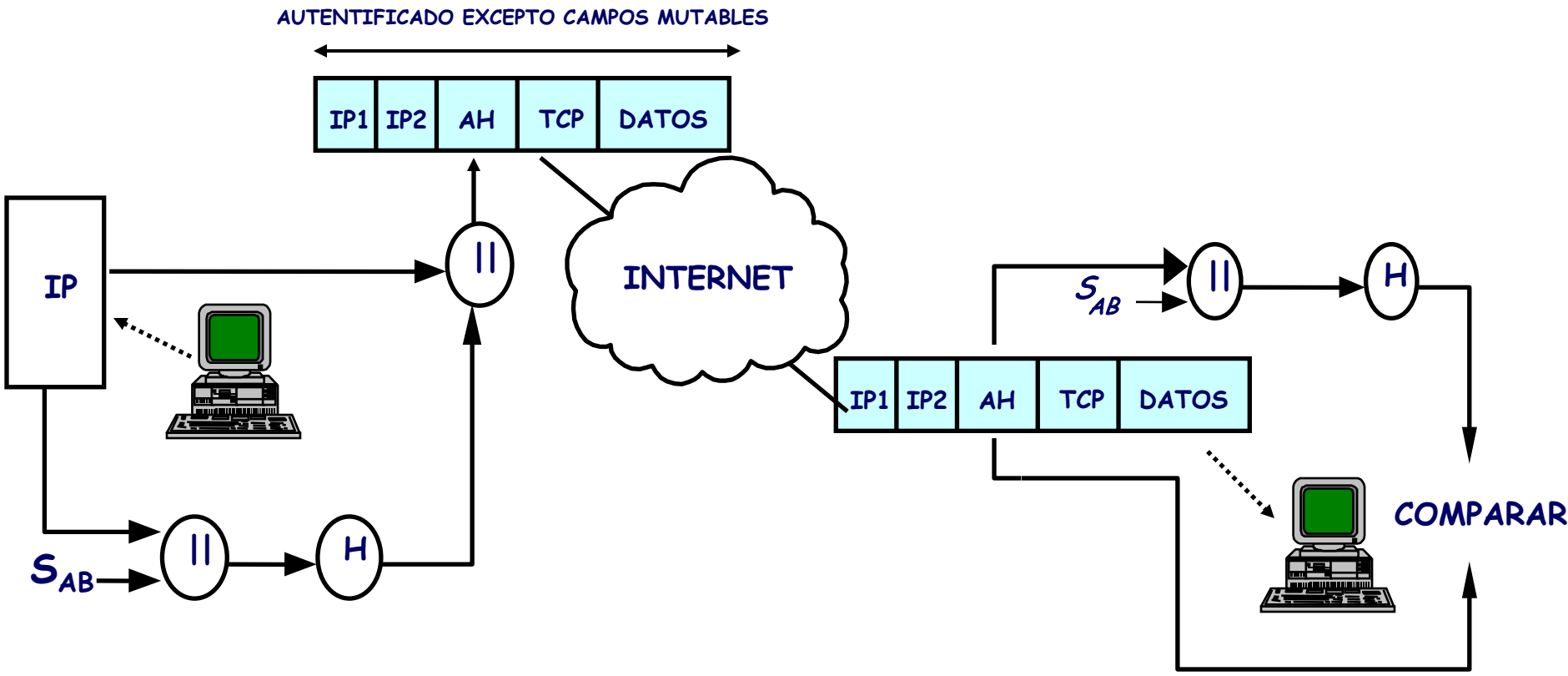


PAQUETE IPSEC MODO TRANSPORTE

ESP: Encapsulation Security Payload

IPSEC:

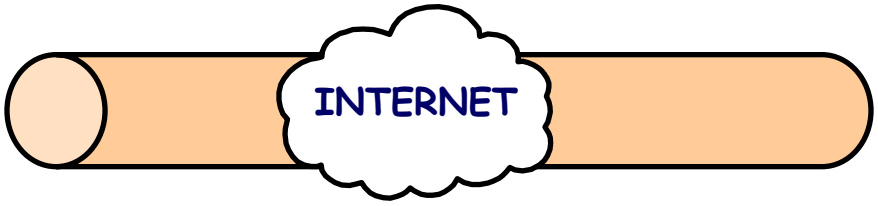
AUTENTICACIÓN MODO TRANSPORTE



AH: Authentication Header

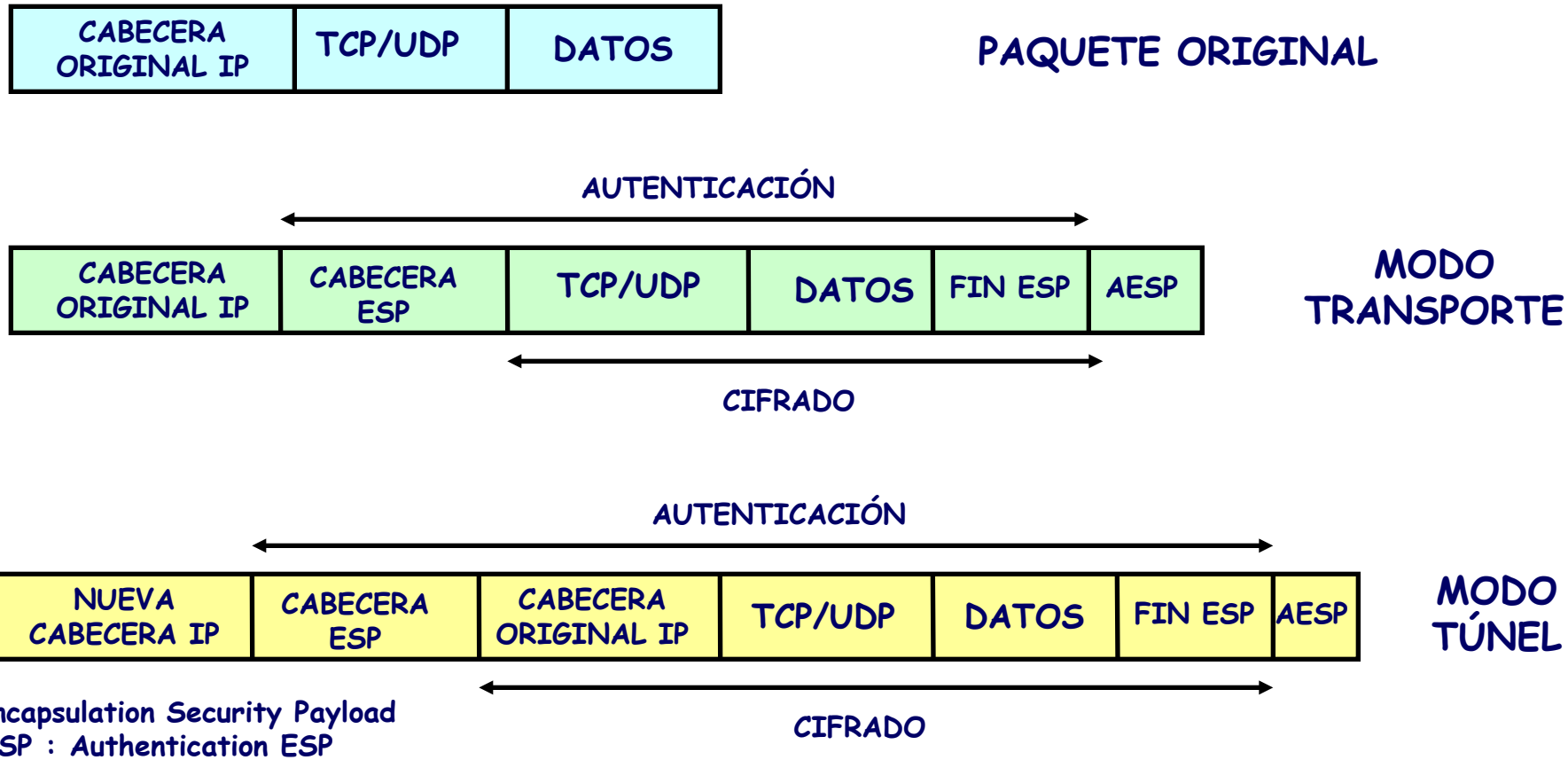
IPSEC:

AUTENTICACIÓN MODO TÚNEL



AH: Authentication Header

IPSEC:
Confidencialidad /Autenticación



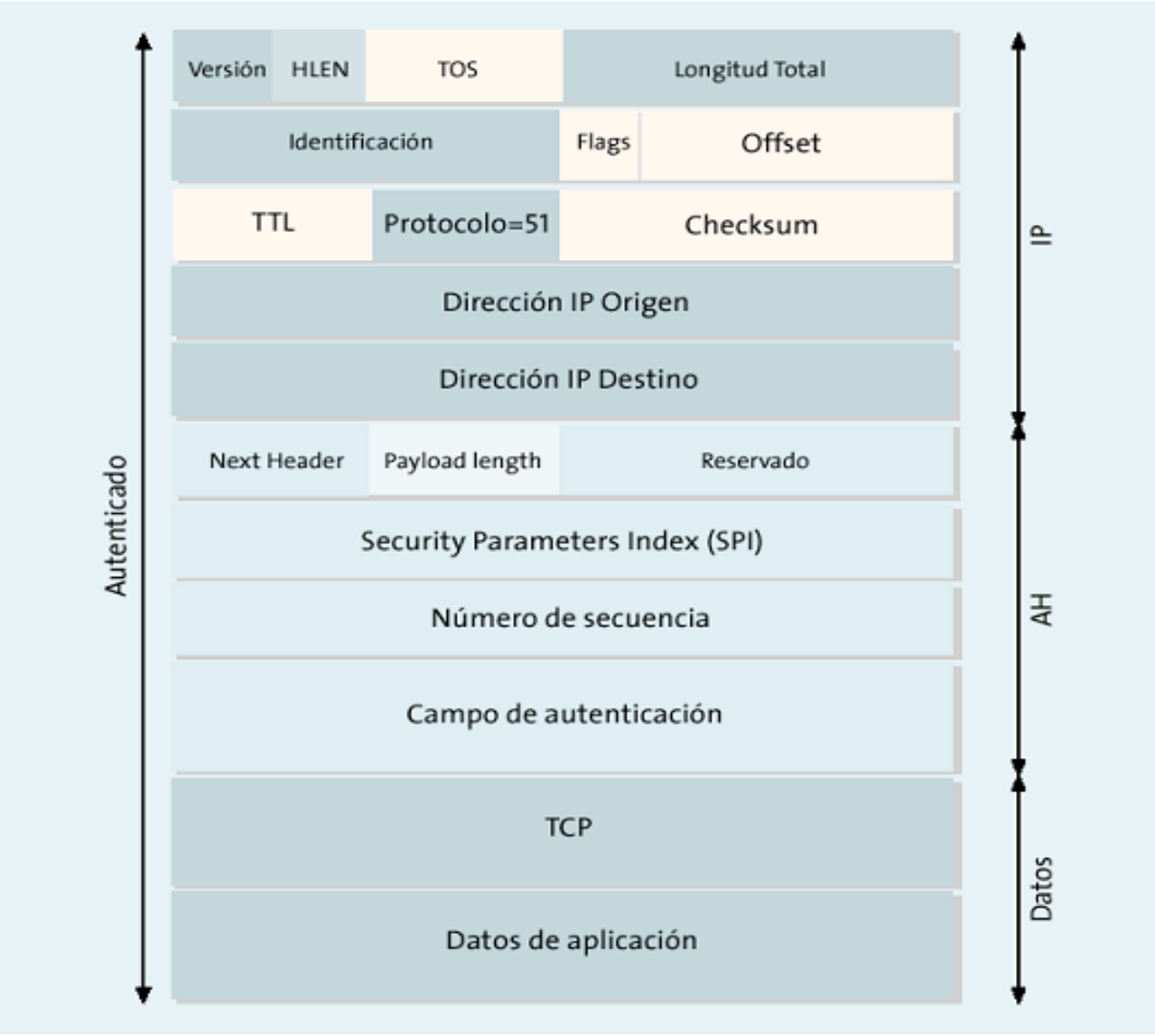
ESP: Encapsulation Security Payload
AESP : Authentication ESP

IPSEC/IPV6
AUTHENTICATION HEADER

BITS

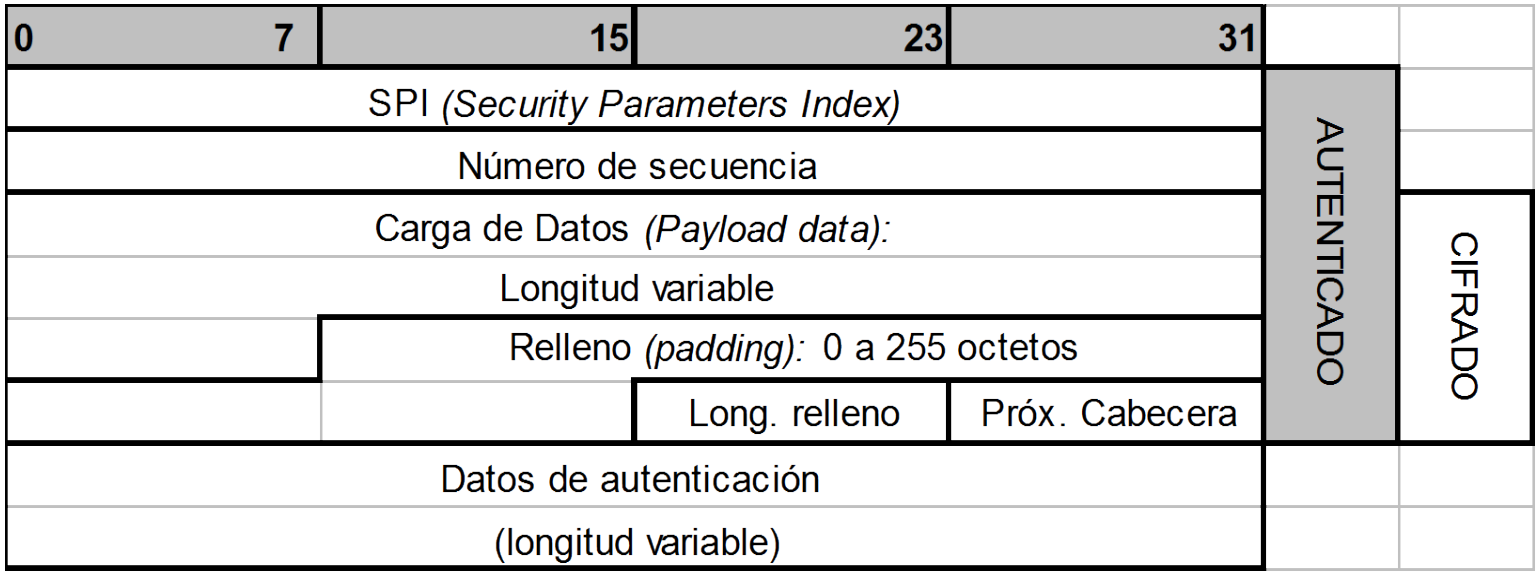
0 7	15	23	31
Próx. Cabecera	Long. Datos	RESERVADO	
SPI *(Security Parameters Index)*			
Número de secuencia			
Datos de autenticación			
(longitud variable)			

IPSEC-IPV4 (AH)

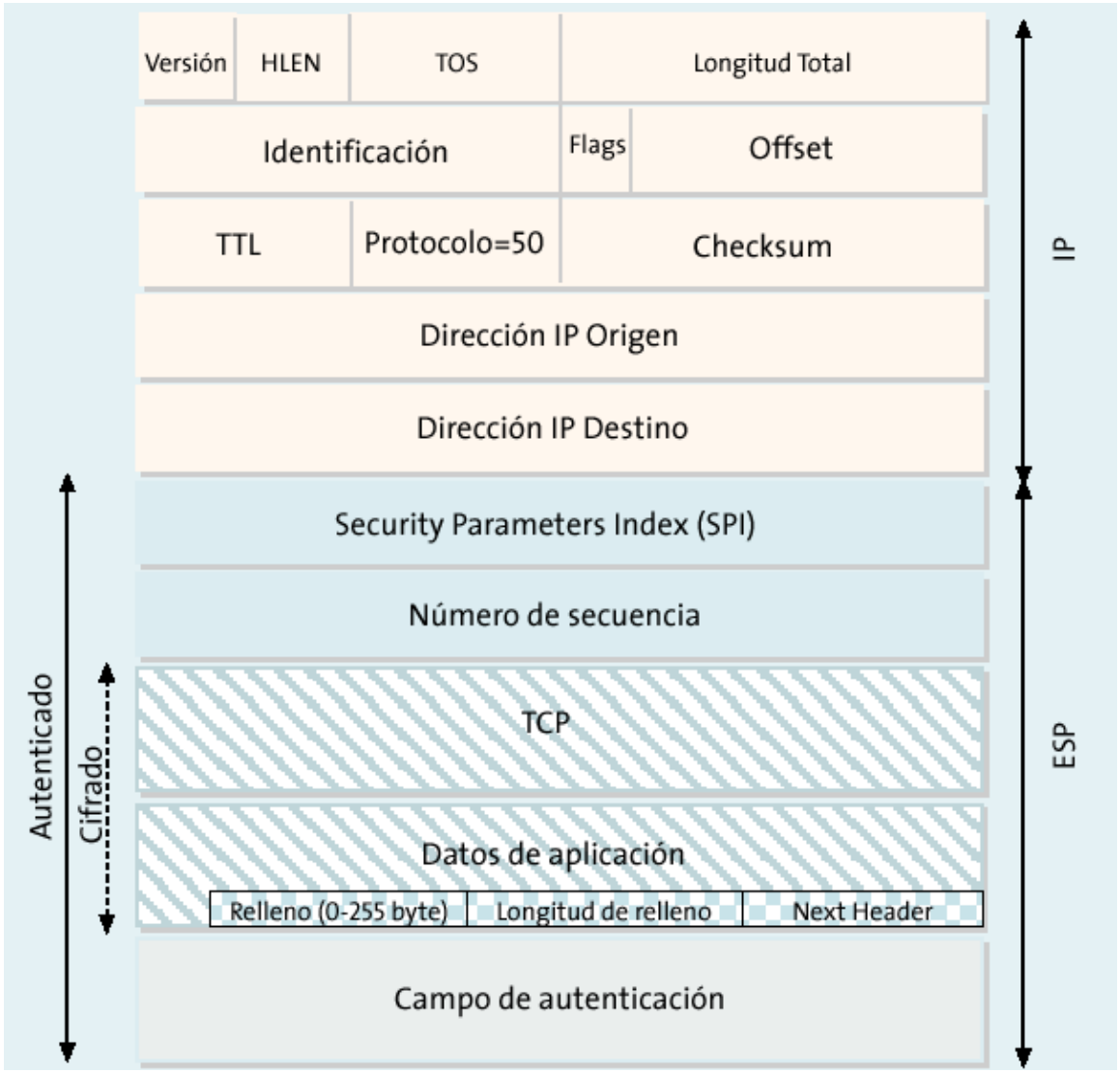


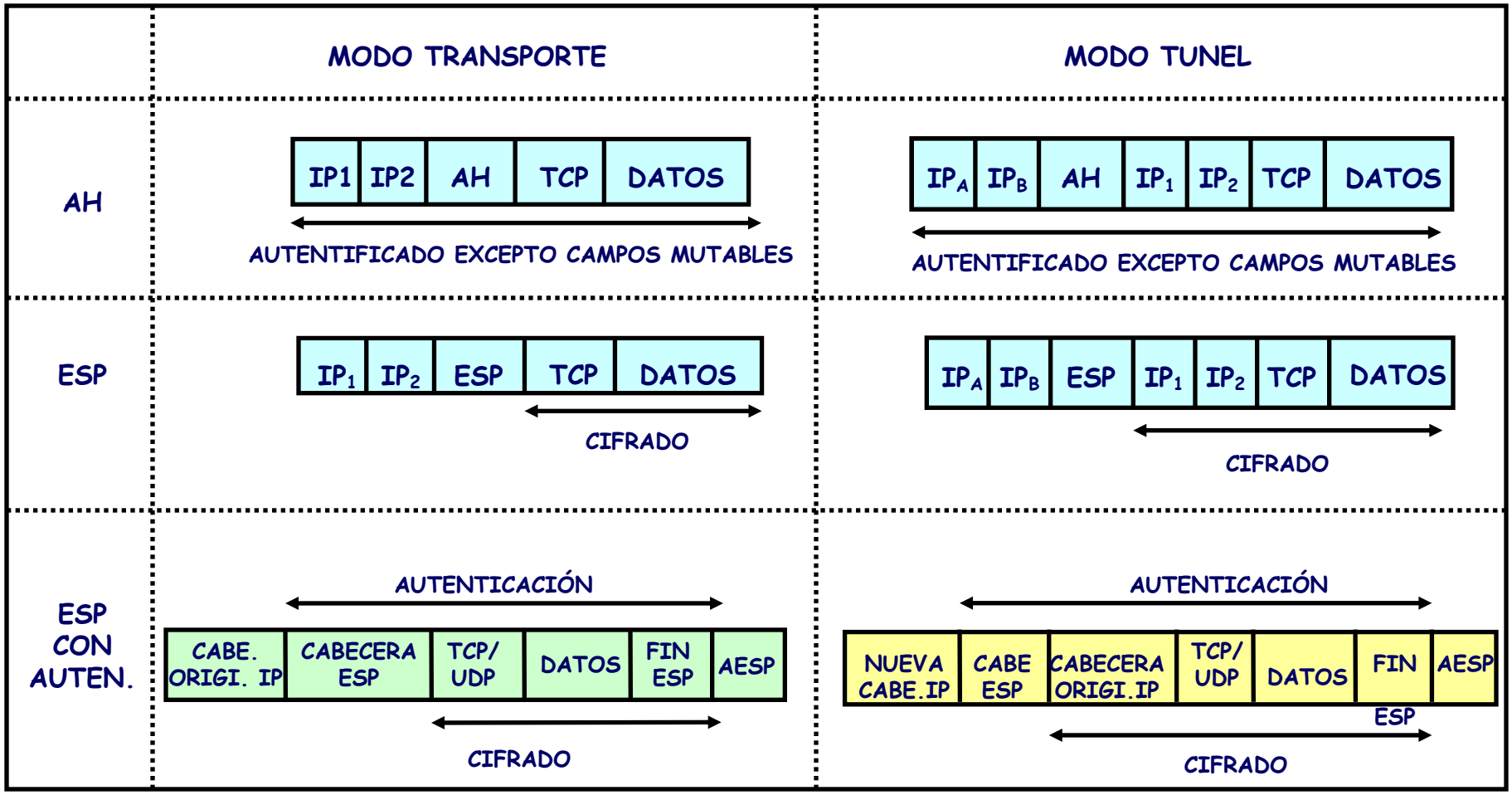
IPSEC/IPV6
Encapsulation Security Payload

BITS

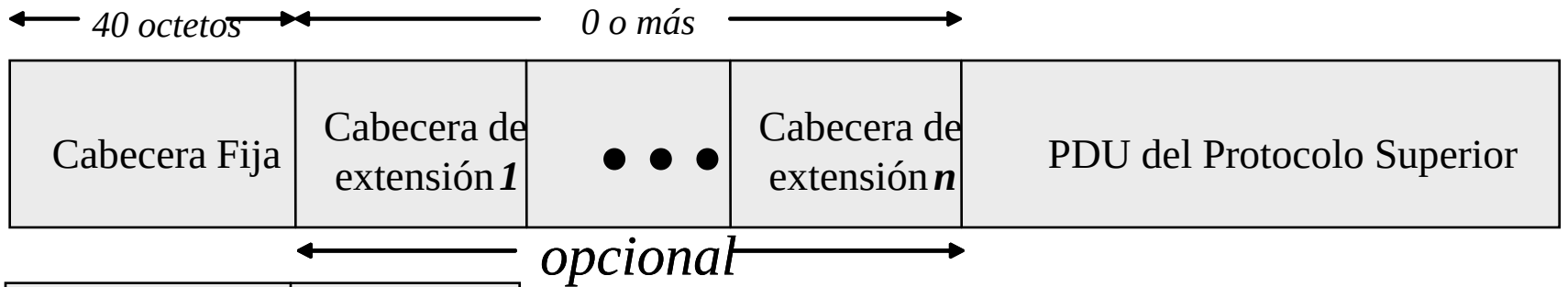


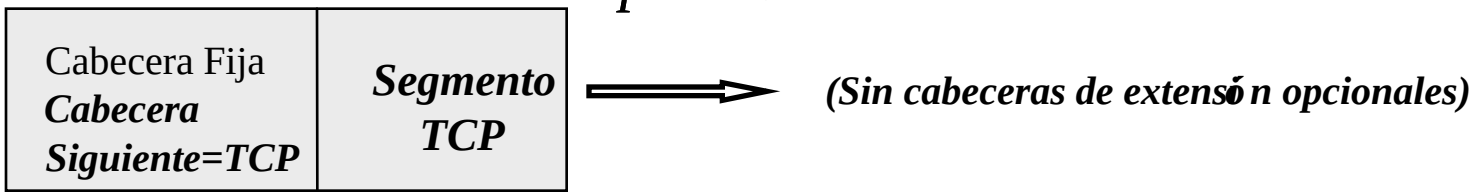
IPSEC-IPV4 (ESP)

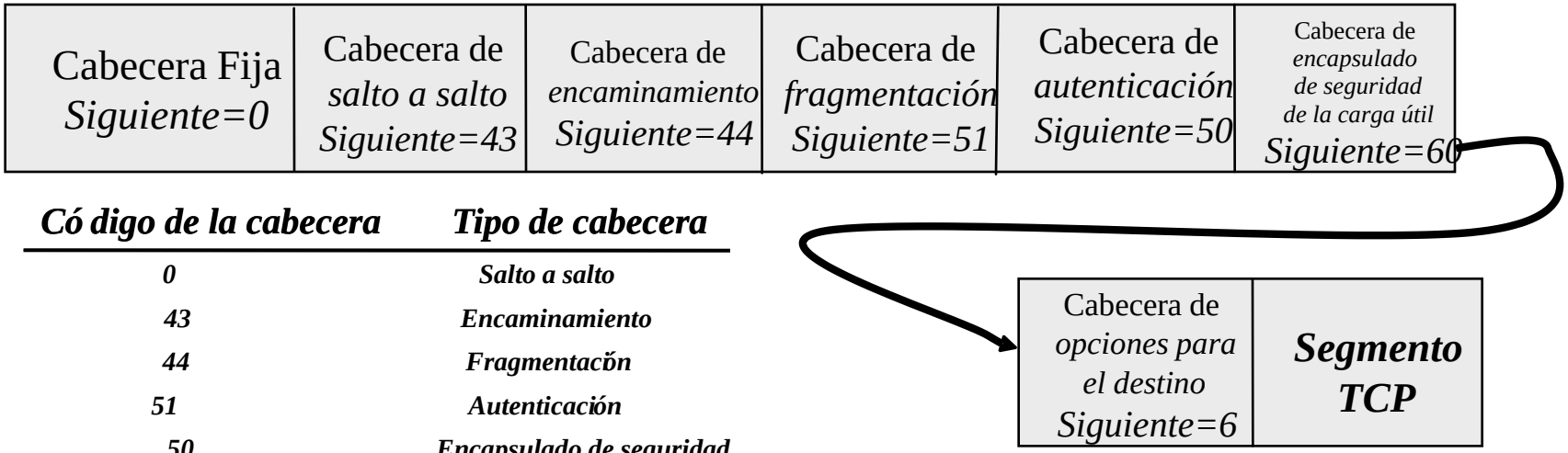



MODO TRANSPORTE
MODO TUNEL
AH
IP1 IP2 AH TCP DATOS
AUTENTIFICADO EXCEPTO CAMPOS MUTABLES
IP$_A$ IP$_B$ AH IP$_1$ IP$_2$ TCP DATOS
AUTENTIFICADO EXCEPTO CAMPOS MUTABLES
ESP
IP$_1$ IP$_2$ ESP TCP DATOS
CIFRADO
IP$_A$ IP$_B$ ESP IP$_1$ IP$_2$ TCP DATOS
CIFRADO
ESP CON AUTEN.
AUTENTICACIÓN
CABE. ORIGI. IP
CABECERA ESP
TCP/ UDP
DATOS
FIN ESP
AESP
CIFRADO
AUTENTICACIÓN
NUEVA CABE.IP
CABE ESP
CABECERA ORIGI.IP
TCP/ UDP
DATOS
FIN
AESP
ESP
CIFRADO

IPV6 (AH-ESP)

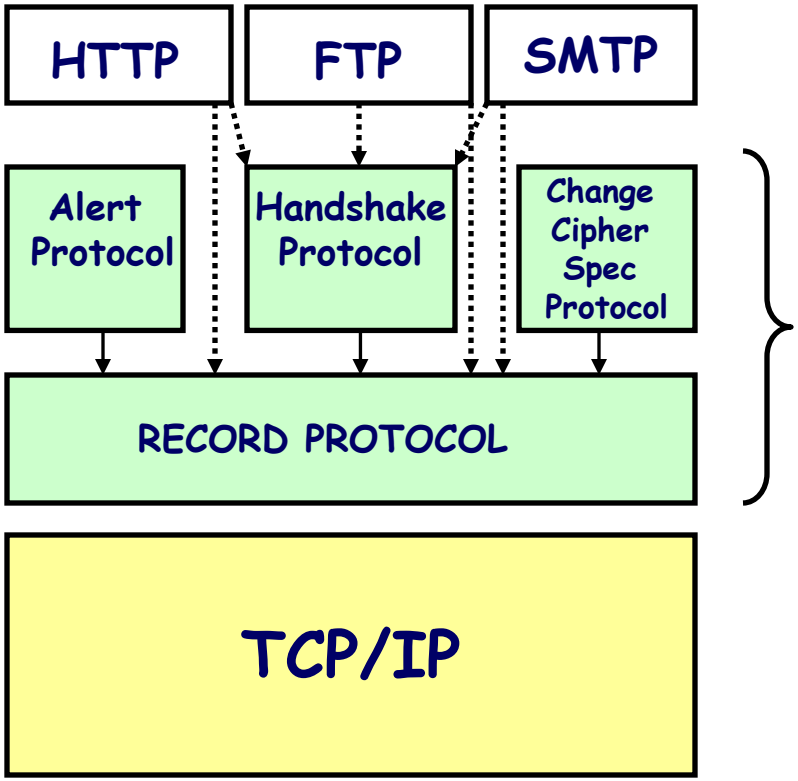






Código de la cabecera	Tipo de cabecera
0	Salto a salto
43	Encaminamiento
44	Fragmentación
51	Autenticación
50	Encapsulado de seguridad de la carga útil
60	Opciones para el destino

SEGURIDAD EN EL NIVEL DE TRANSPORTE



SECURE SOCKETS LAYER, SSL (I)

- Capa de seguridad adicional en la pila TCP/IP transparente a las aplicaciones
- El objetivo es proporcionar servicios de seguridad en Internet:
  - Autenticación de un Servidor:
  - Autenticación de un Cliente
  - Conexión cifrada segura cliente-servidor (confidencialidad)
  - Integridad y autenticación datos

SECURE SOCKETS LAYER, SSL(II)

- SSL incluye dos sub-protocolos básicos:
  - Protocolo de Seguridad (Handshake Protocol)
  - Protocolo de transporte (Record Protocol)
- SSL incluye dos sub-protocolos adicionales:
  - Protocolo de notificación de alertas (Alert Protocol)
  - Protocolo de notificación actualización de cifradores (Change Cipher Spec Protocol)

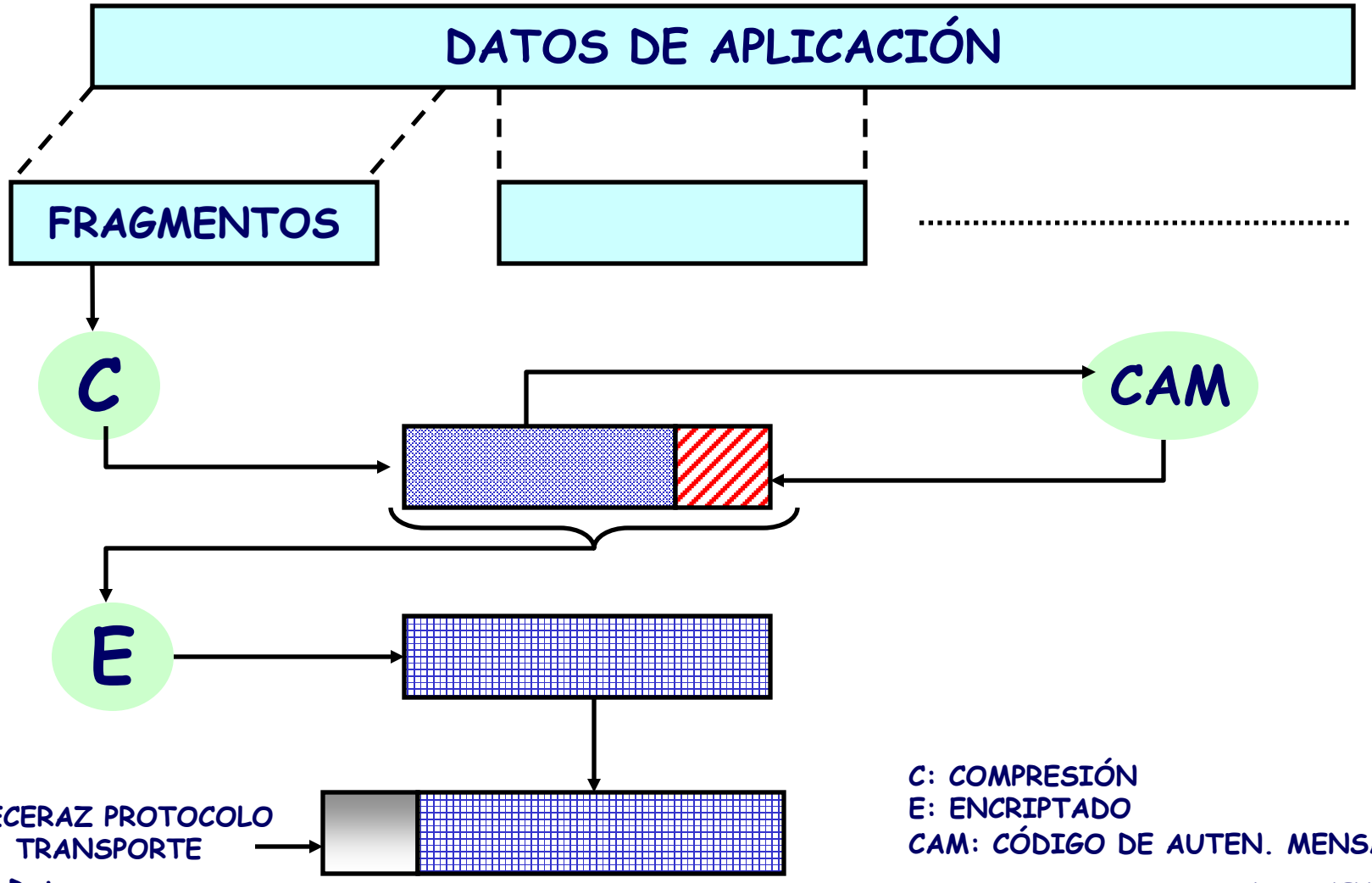
SESIÓN - CONEXIÓN SSL

- Sesión SSL:
  - Identificador de sesión, Método de Compresión, Cifradores, "Master Secret",...
- Conexión SSL:
  - Claves CAM del Cliente y Servidor, Claves de Sesión del Cliente y Servidor, Números de secuencia...

PROTOCOLO DE TRANSPORTE (I) (Record Protocol)

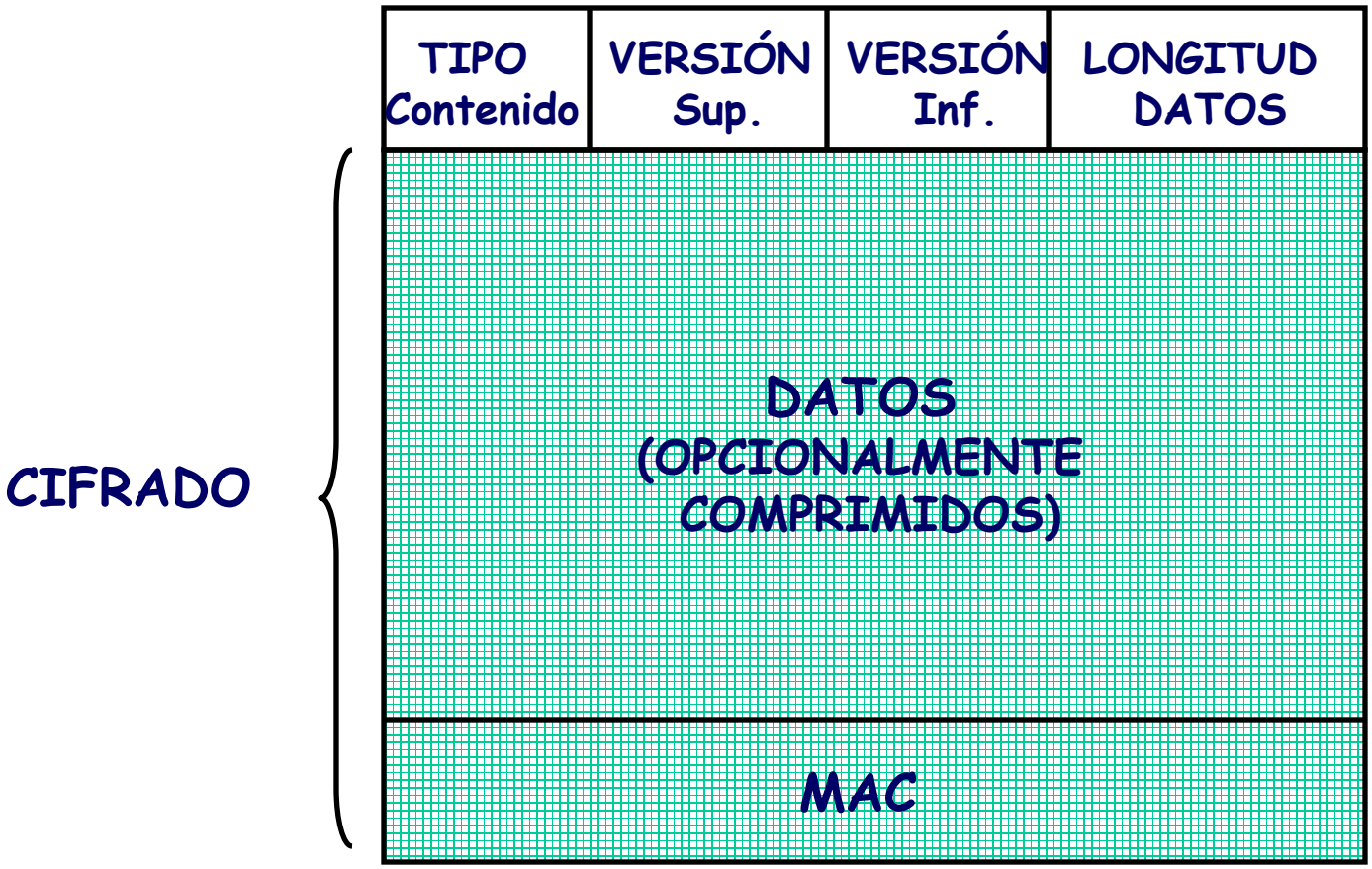
- Proporciona dos servicios a las conexiones SSL:
  - Confidencialidad
    - El protocolo de Autenticación define las claves de sesión usadas en el cifrado/descifrado
  - Integridad
    - El protocolo de Autenticación define la clave secreta utilizada en un Código de Autenticación de Mensajes

PROTOCOLO DE TRANSPORTE (II)
(Record Protocol)



C: COMPRESIÓN
E: ENCRIPTADO
CAM: CÓDIGO DE AUTEN. MENSAJES

PROTOCOLO DE TRANSPORTE (III)
(Record Protocol)



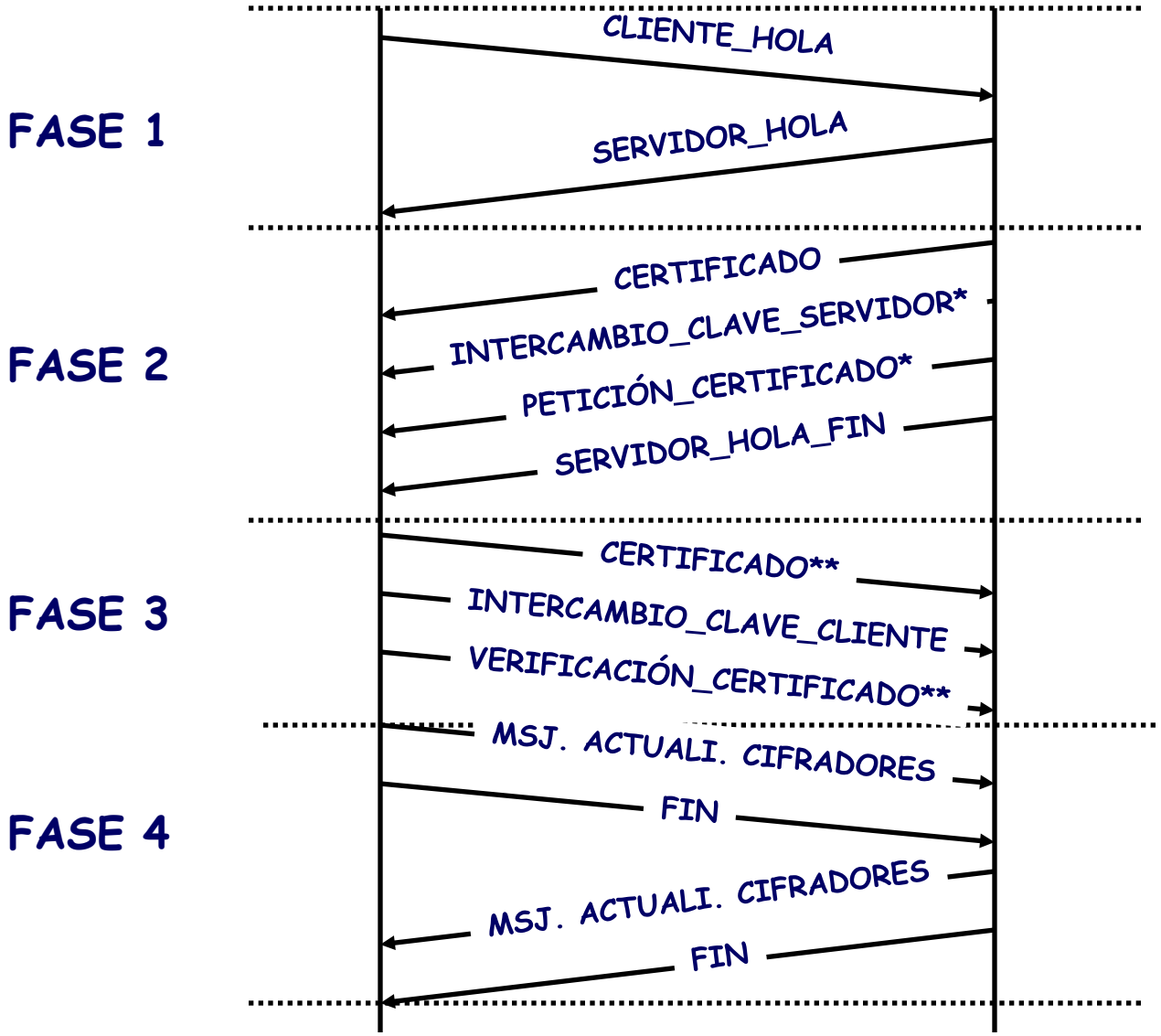
PROTOCOLO DE SEGURIDAD (I) (Handshake Protocol)

- EL Protocolo de Seguridad permite:
  - Autentificarse mutuamente cliente y servidor
  - Negociar los algoritmos de Cifrado y MAC
  - Intercambiar las claves necesarias para proteger los datos
- EL Protocolo de Seguridad utiliza una conjunto de mensajes:
  - Los mensaje tiene tres campos:
    - Tipo(1byte), Longitud (3bytes), parámetros (>=0 byte)
  - Tipos de mensajes:
    - client_hello,server_hello, certificate, change_cipher_spec .....

PROTOCOLO DE SEGURIDAD (II)

- EL Protocolo de Seguridad consta de cuatro fases:
  - Fase 1: Establecimiento de los parámetros de la comunicación
  - Fase 2: Autenticación del servidor
  - Fase 3: Autenticación del cliente e intercambio de clave de sesión
  - Fase 4: Fase final

PROTOCOLO DE AUTENTICACIÓN (III)



FASE 1:Establecimiento Párametros de la Comunicación

- Mensaje "*Client_Hello*":
  - Versión SSL
  - Número Aleatorio
  - Identificador de sesión
  - Familia de Cifradores soportados por el cliente
  - Métodos de compresión soportados por el cliente
- Mensaje "*Server_Hello*":
  - Mismos parámetros que el mensaje "Client_Hello"
  - El servidor selecciona la familia de cifradores y métodos de compresión de entre los propuestos por el cliente

FAMILIA DE CIFRADORES

- Métodos de intercambio de clave
  - RSA (el más utilizado
  - Diffie-Hellman (dintintas variantes)
- Algoritmos de cifrado
  - RC4, RC2, DES, 3DES, IDEA, AES
- Funciones Hash
  - MD5, SHA,....
- .....

FASE 2:Autenticación del servidor (I)

- Mensaje "*Certificate*":
  - Certificado de clave pública X.509 del servidor firmado por una CA.
  - Esta clave será utilizada para intercambiar una clave de sesión
- Mensaje "*Server_Key_Interchange*" (opcional):
  - El servidor puede crear un par de claves pública/secreta temporales.
  - En este mensaje envía al cliente un certificado de la clave pública

FASE 2:Autenticación del servidor (II)

- Mensaje "*Certificate_Request*" (opcional):
  - El servidor puede pedir un certificado al cliente
  - El mensaje incluye el tipo de certificado y una lista de autoridades de certificación aceptables
- Mensaje "*Server_done*":
  - Este mensaje no tiene parámetros
  - En este mensaje indica el fin de los mensajes asociados al servidor

FASE 3:Autenticación del cliente e intercambio de clave (I)

- Mensaje *"Certificate"* (obligatorio si es solicitado por el servidor):
  - El cliente envía un certificado al servidor si éste se lo solicitó
- Mensaje *"Client_key_exchange"*:
  - El cliente genera una pre-master secret de 48 bytes cifrada con la clave pública del servidor
  - El cliente y el servidor utilizan la pre-master secret para generar las claves de sesión y las claves MAC

FASE 3:Autenticación del cliente e intercambio de clave (II)

- Mensaje *"Certificate_Verify"* (obligatorio si es solicitado por el servidor un certificado de cliente):
  - Este mensaje se envía junto con el anterior
  - Consta de una firma Hash que abarca los mensajes anteriores. El cifrado se hace con la clave privada del cliente.

FASE 4: FIN DE LOS INTERCAMBIOS

- Mensaje *"finished"*:
  - Este mensaje se envía después de un mensaje "*change cipher spec*"
  - Es el primer mensaje protegido con las claves y algoritmos recién negociados
  - No se requiere reconocimiento de este mensaje
  - Las entidades puede enviar información confidencial después de enviar este mensaje

PROTOCOLOS ADICIONALES SSL

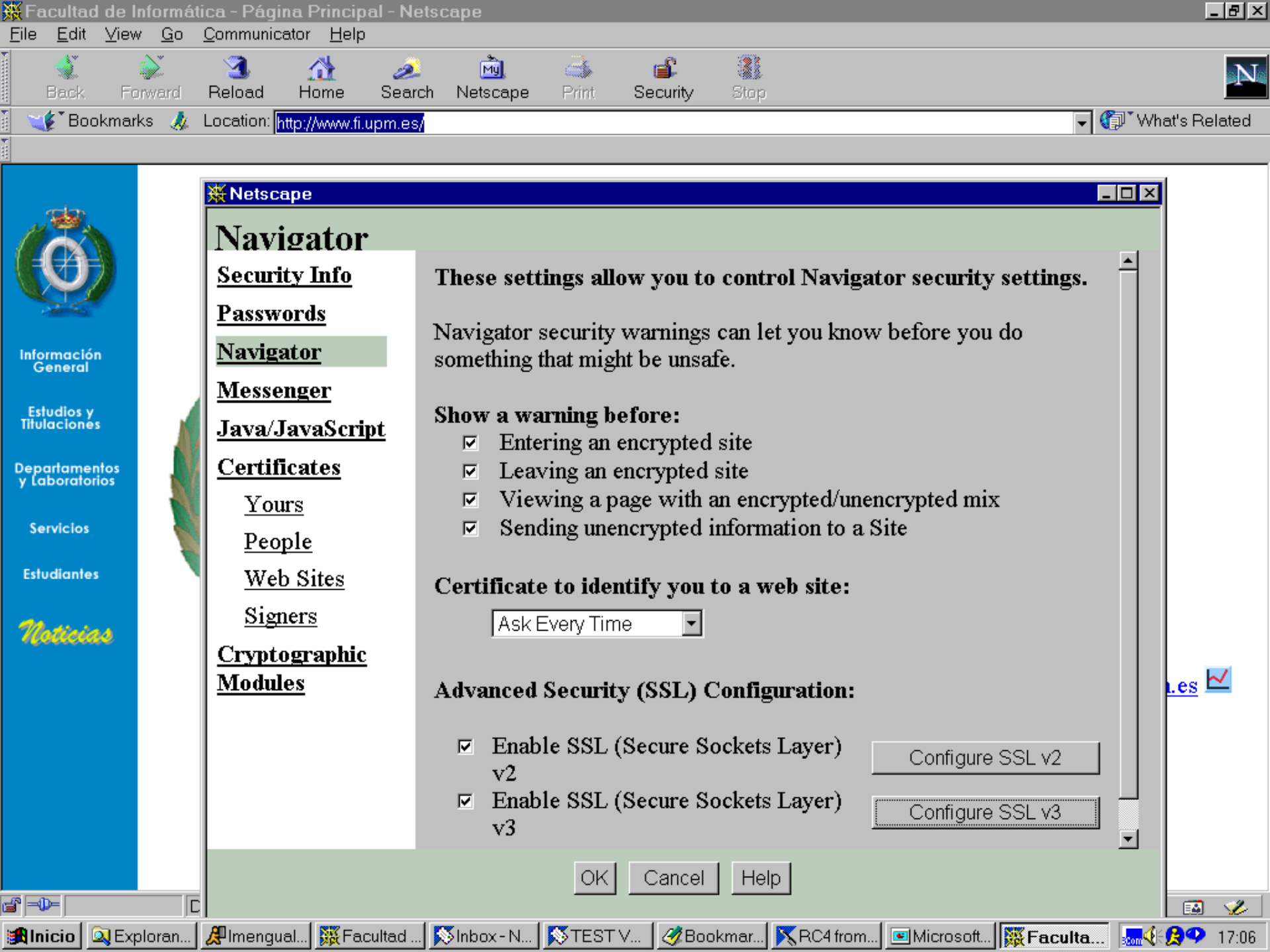
- Protocolo de notificación de alertas (Alert Protocol)
  - Notificación de alertas a las entidades
    - Incorrecto MAC, mensaje inesperado, parámetros ilegales en el protocolo de autenticación, certificados revocados o expirados, error al descomprimir datos...
  - Los mensajes se componen de dos bytes
    - El primer byte indica el nivel de la alerta
    - El segundo byte contiene el código de la alerta

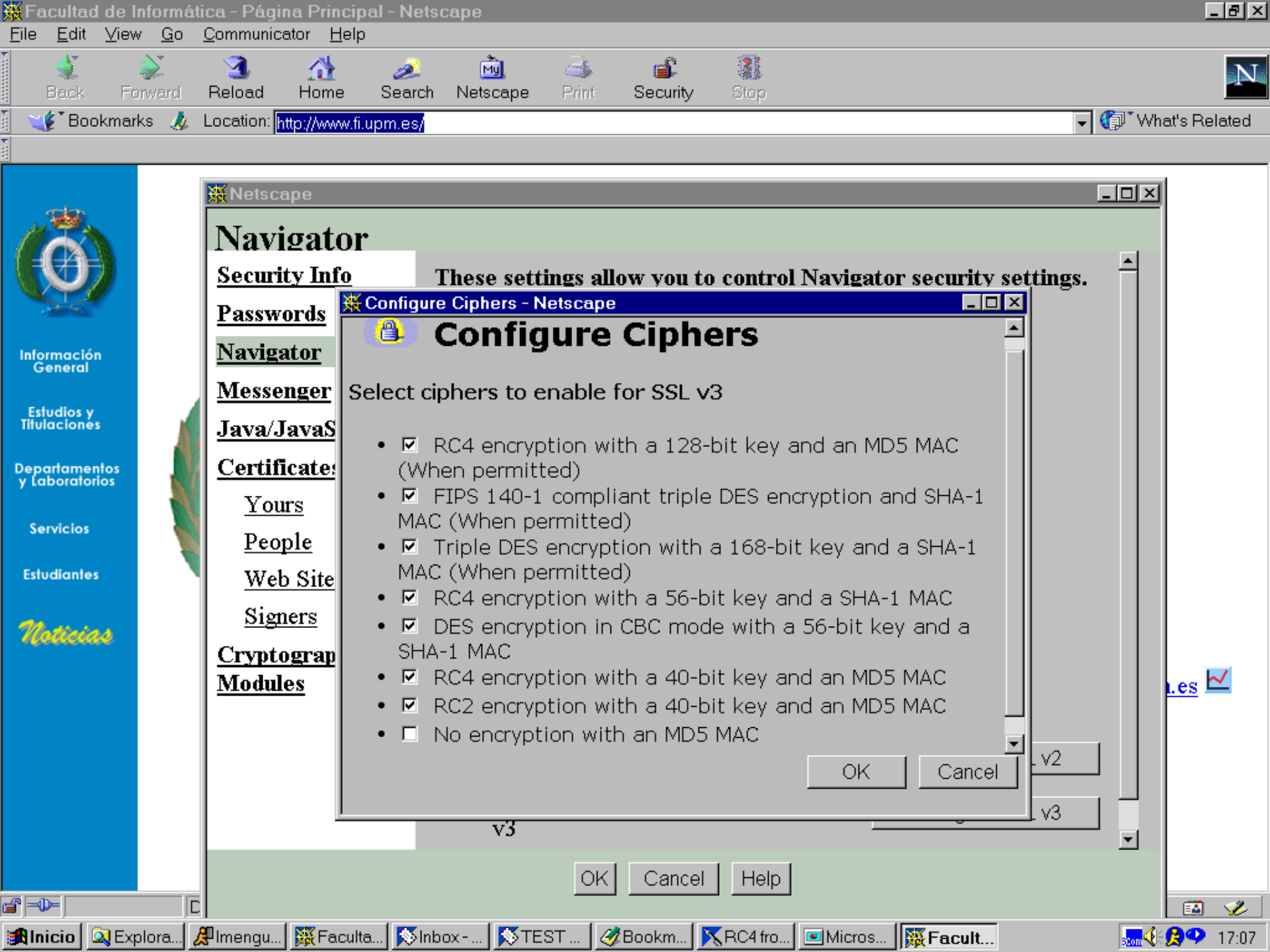
PROTOCOLOS ADICIONALES SSL

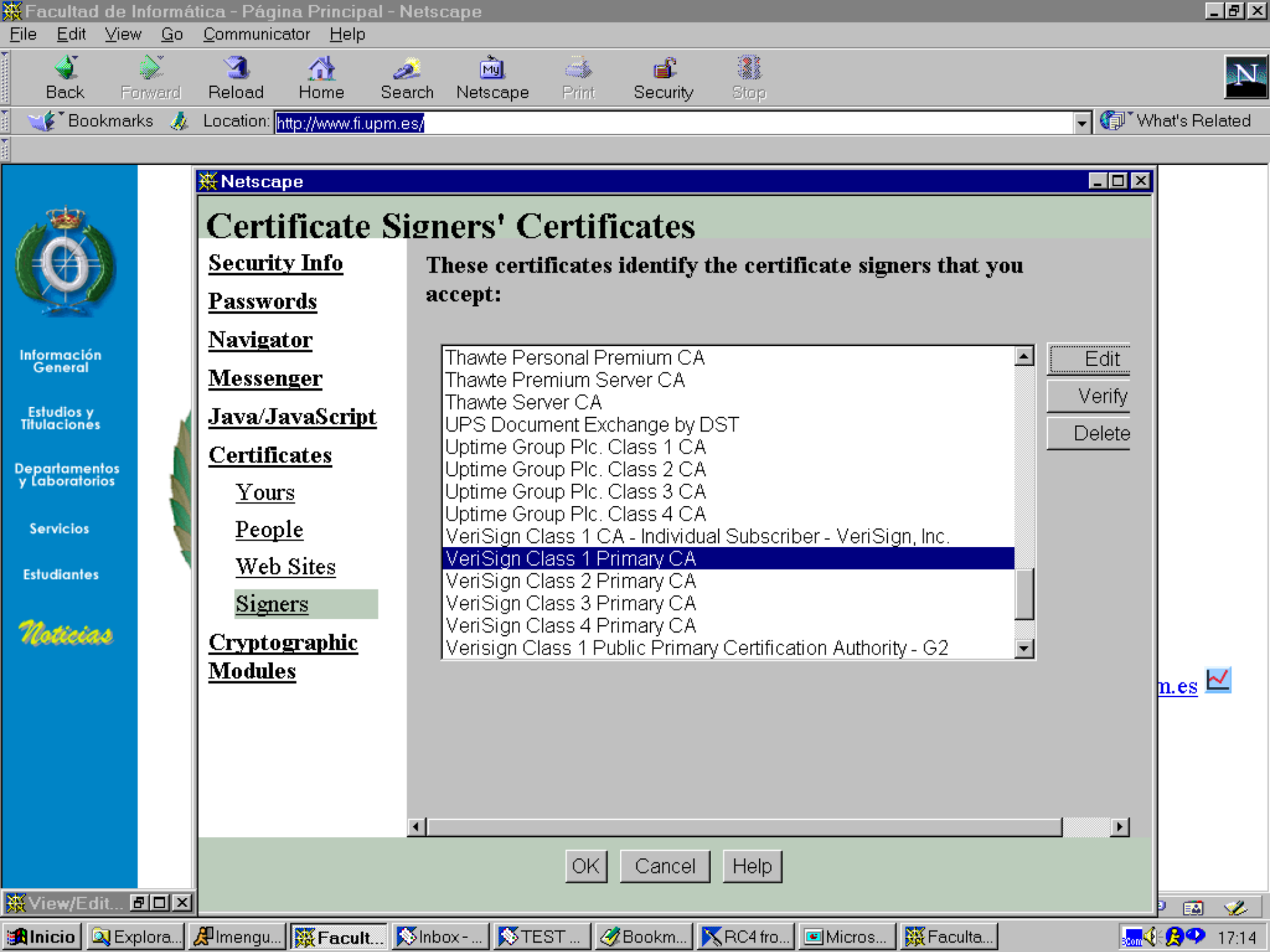
- Protocolo de notificación actualización de cifradores (Change Cipher Spec Protocol)
  - Se trata de un solo mensaje de un solo byte de valor 1
  - El propósito de este mensaje es actualizar los cifradores a utilizar en la conexión

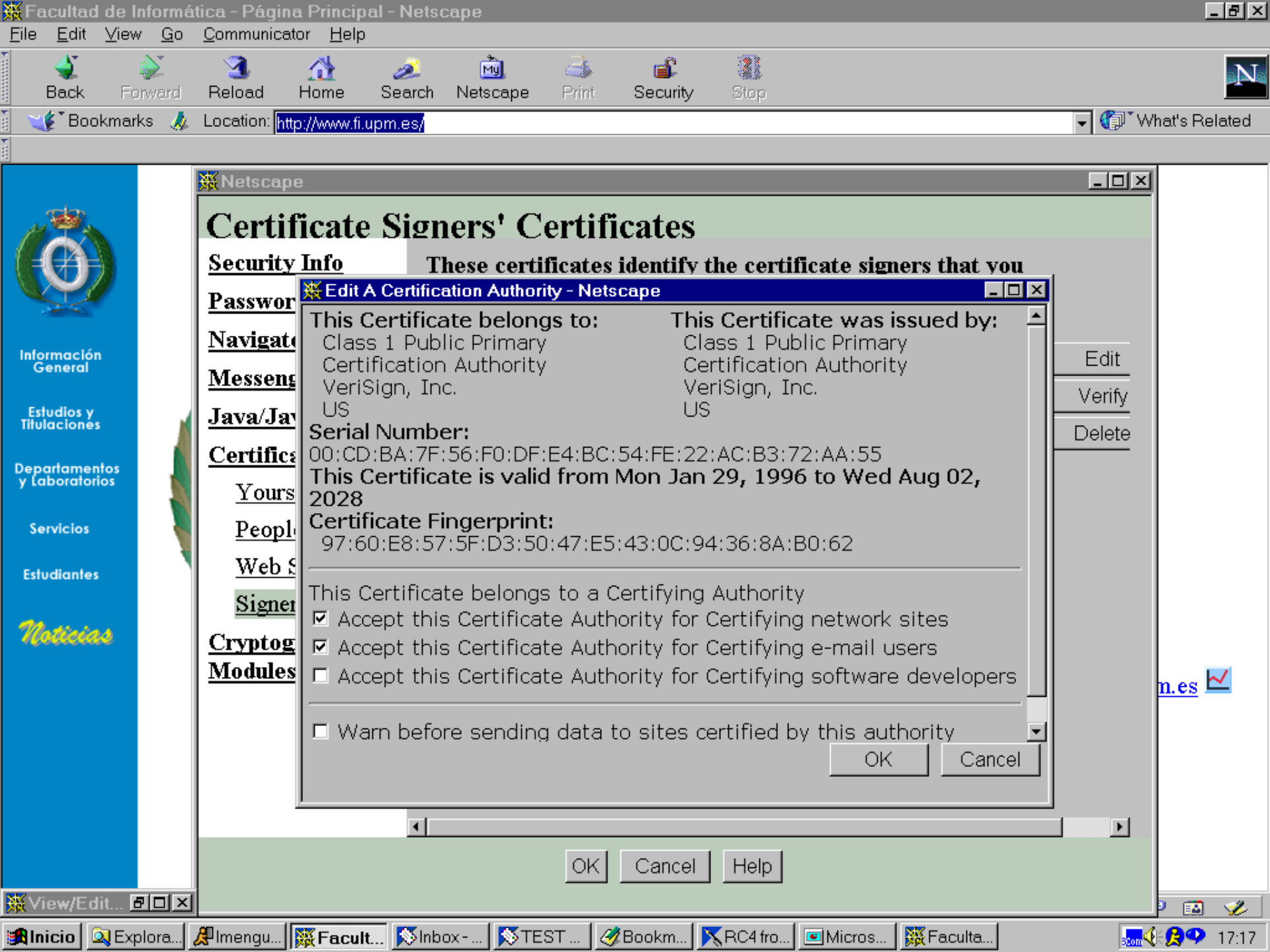
INICIO SESIÓN SSL

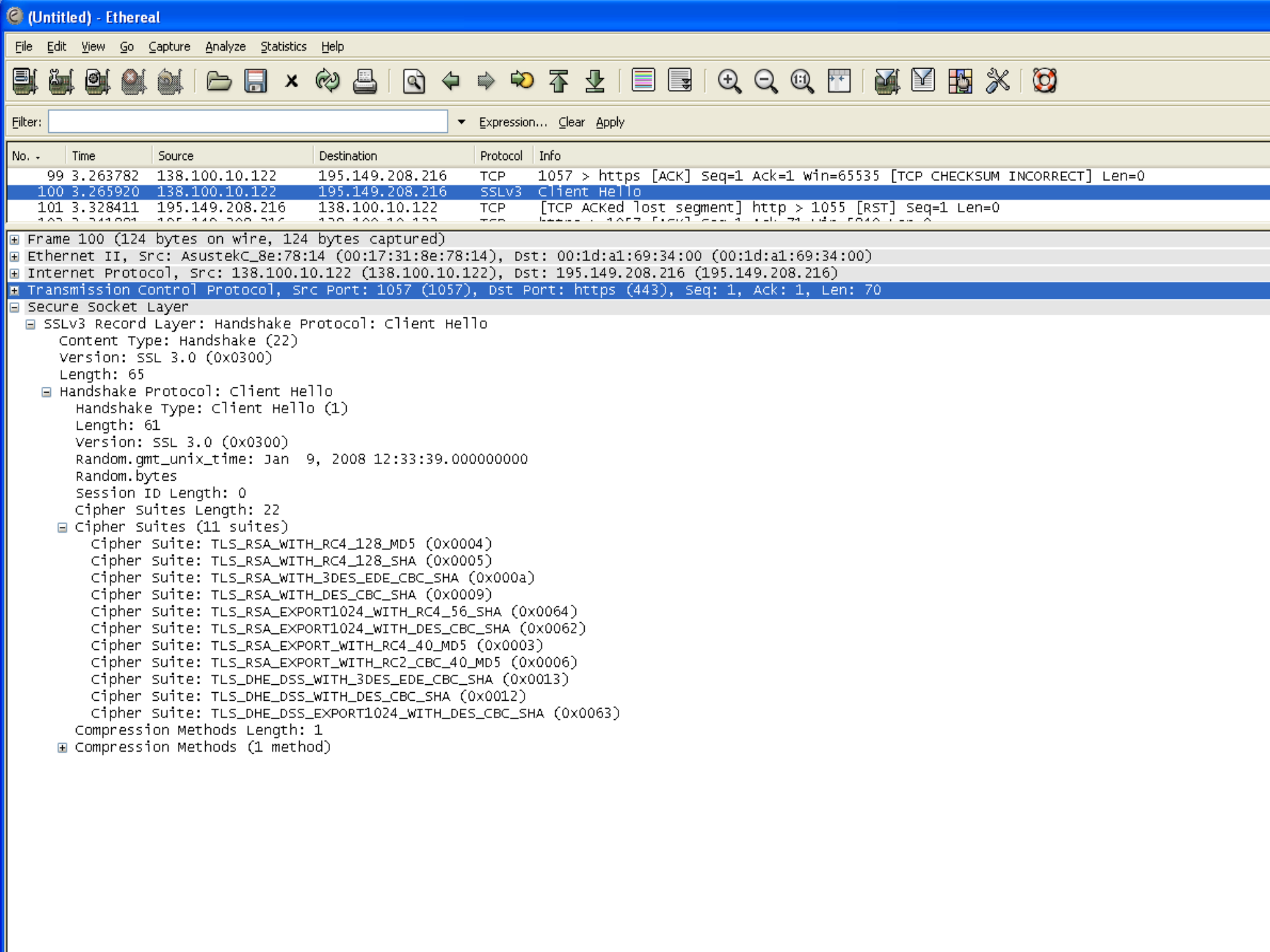
- En el cliente (*navegador*) el usuario pide un documento con una *URL* que comienza con *"https"* en vez de *"http"*
- El código del cliente reconoce la petición *SSL* y establece una conexión a través del *puerto TCP 443* del servidor (en vez del *puerto TCP 80, http*)
- El cliente inicia los intercambios del *Protocolo de Autenticación SSL* utilizando como portador el *Protocolo de Transporte*
  - En un primer momento no hay mecanismos de cifrado ni verificación de la integridad en la conexión *TCP*

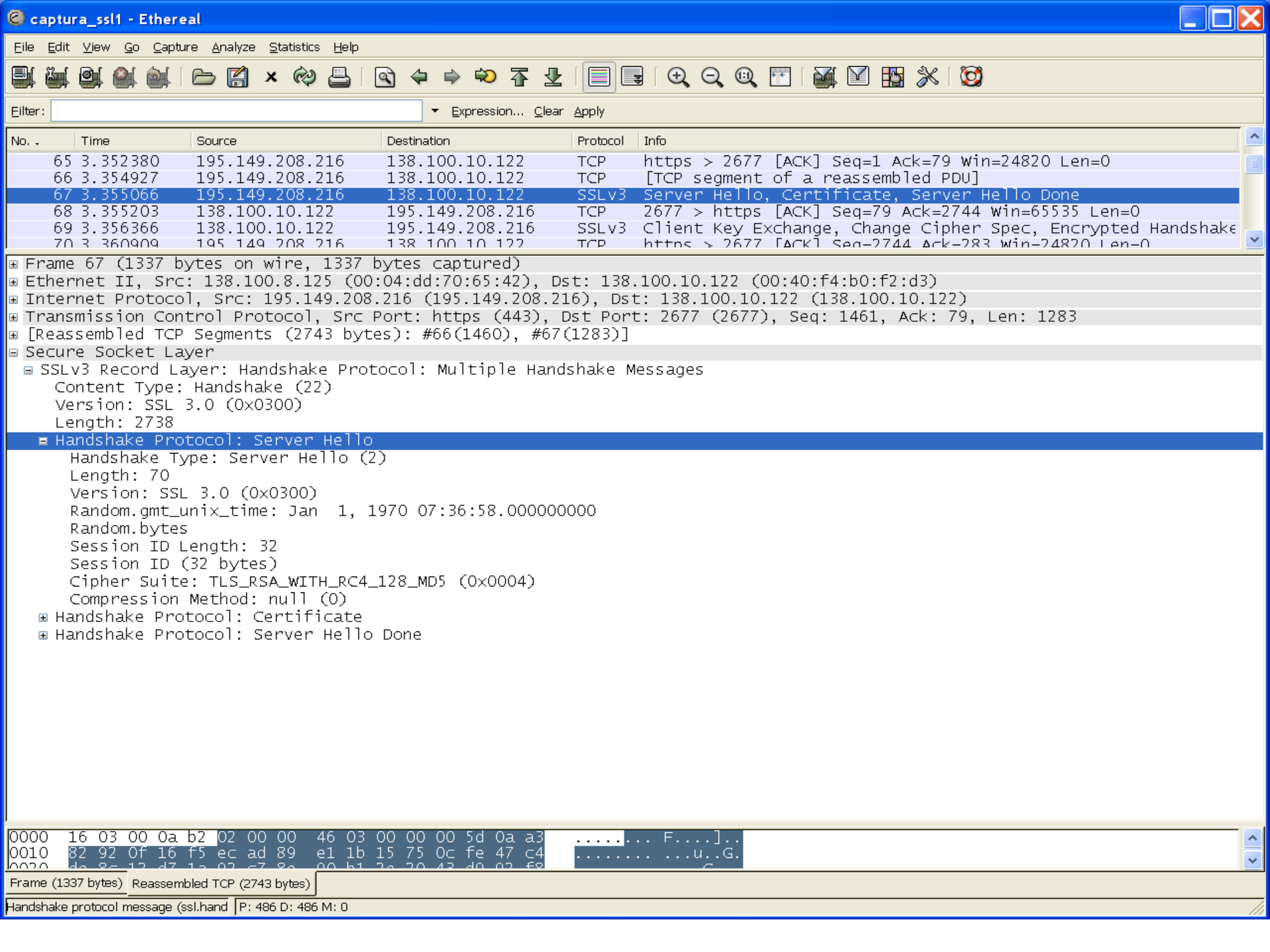

Facultad de Informática - Página Principal - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Stop
Bookmarks Location: http://www.fi.upm.es/ What's Related
Información General
Estudios y Titulaciones
Departamentos y Laboratorios
Servicios
Estudiantes
Noticias
Netscape
Navigator
Security Info
Passwords
Navigator
Messenger
Java/JavaScript
Certificates
Yours
People
Web Sites
Signers
Cryptographic Modules
These settings allow you to control Navigator security settings.
Navigator security warnings can let you know before you do something that might be unsafe.
Show a warning before:
Entering an encrypted site
Leaving an encrypted site
Viewing a page with an encrypted/unencrypted mix
Sending unencrypted information to a Site
Certificate to identify you to a web site:
Ask Every Time
Advanced Security (SSL) Configuration:
Enable SSL (Secure Sockets Layer) v2
Configure SSL v2
Enable SSL (Secure Sockets Layer) v3
Configure SSL v3
OK Cancel Help
Inicio Exploran... Imengual... Facultad ... Inbox - N... TEST V... Bookmar... RC4 from... Microsoft... Faculta... 17:06

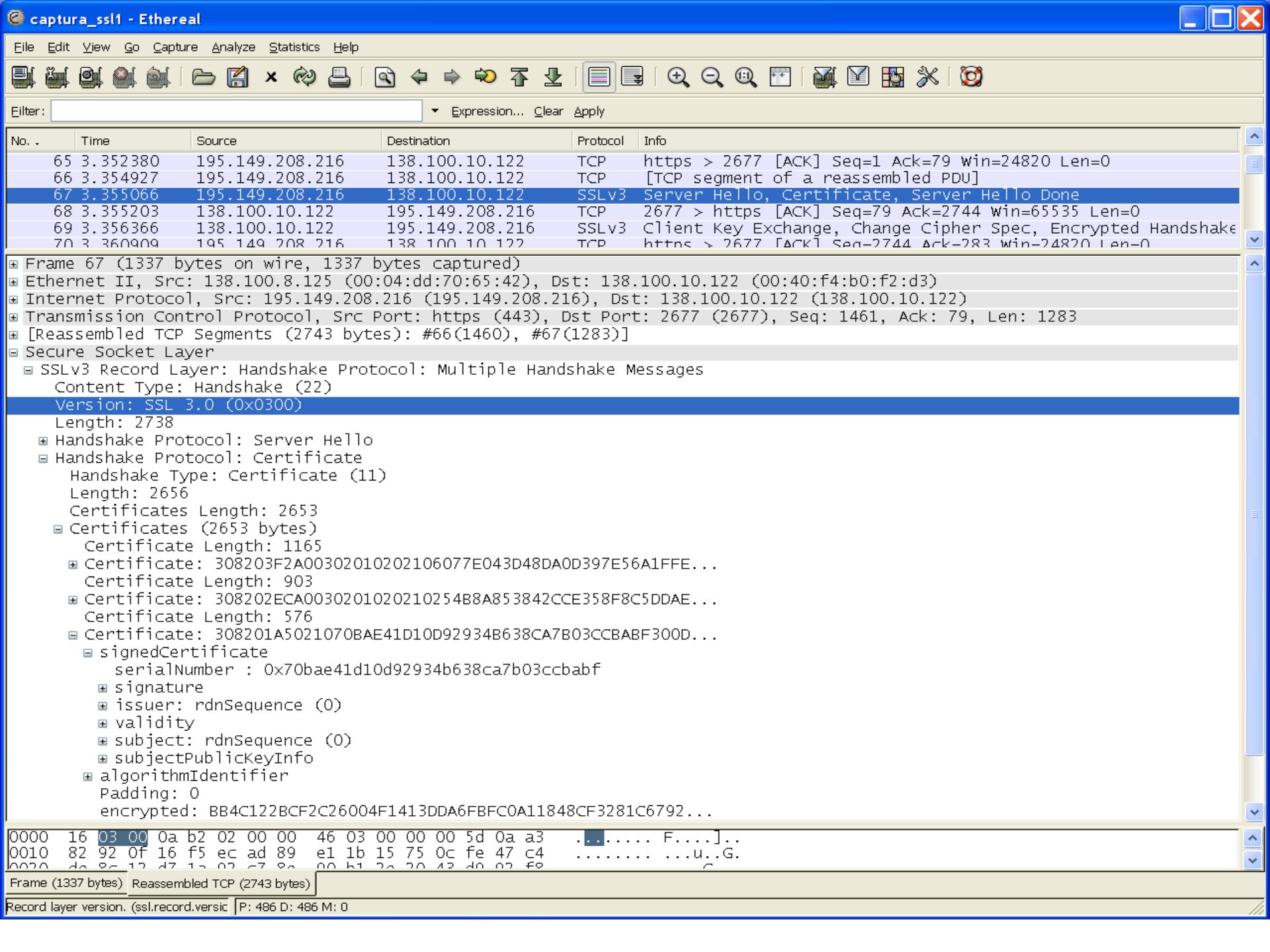

Facultad de Informática - Página Principal - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Stop
Bookmarks Location: http://www.fi.upm.es/
What's Related
Información General
Estudios y Titulaciones
Departamentos y Laboratorios
Servicios
Estudiantes
Noticias
Netscape
Navigator
Security Info
Passwords
Navigator
Messenger
Java/JavaS
Certificates
Yours
People
Web Site
Signers
Cryptograp
Modules
These settings allow you to control Navigator security settings.
Configure Ciphers - Netscape
Configure Ciphers
Select ciphers to enable for SSL v3
RC4 encryption with a 128-bit key and an MD5 MAC (When permitted)
FIPS 140-1 compliant triple DES encryption and SHA-1 MAC (When permitted)
Triple DES encryption with a 168-bit key and a SHA-1 MAC (When permitted)
RC4 encryption with a 56-bit key and a SHA-1 MAC
DES encryption in CBC mode with a 56-bit key and a SHA-1 MAC
RC4 encryption with a 40-bit key and an MD5 MAC
RC2 encryption with a 40-bit key and an MD5 MAC
No encryption with an MD5 MAC
OK
Cancel
v2
v3
v3
OK
Cancel
Help
Inicio
Explora...
Imengu...
Faculta...
Inbox - ...
TEST ...
Bookm...
RC4 fro...
Micros...
Facult...
17:07

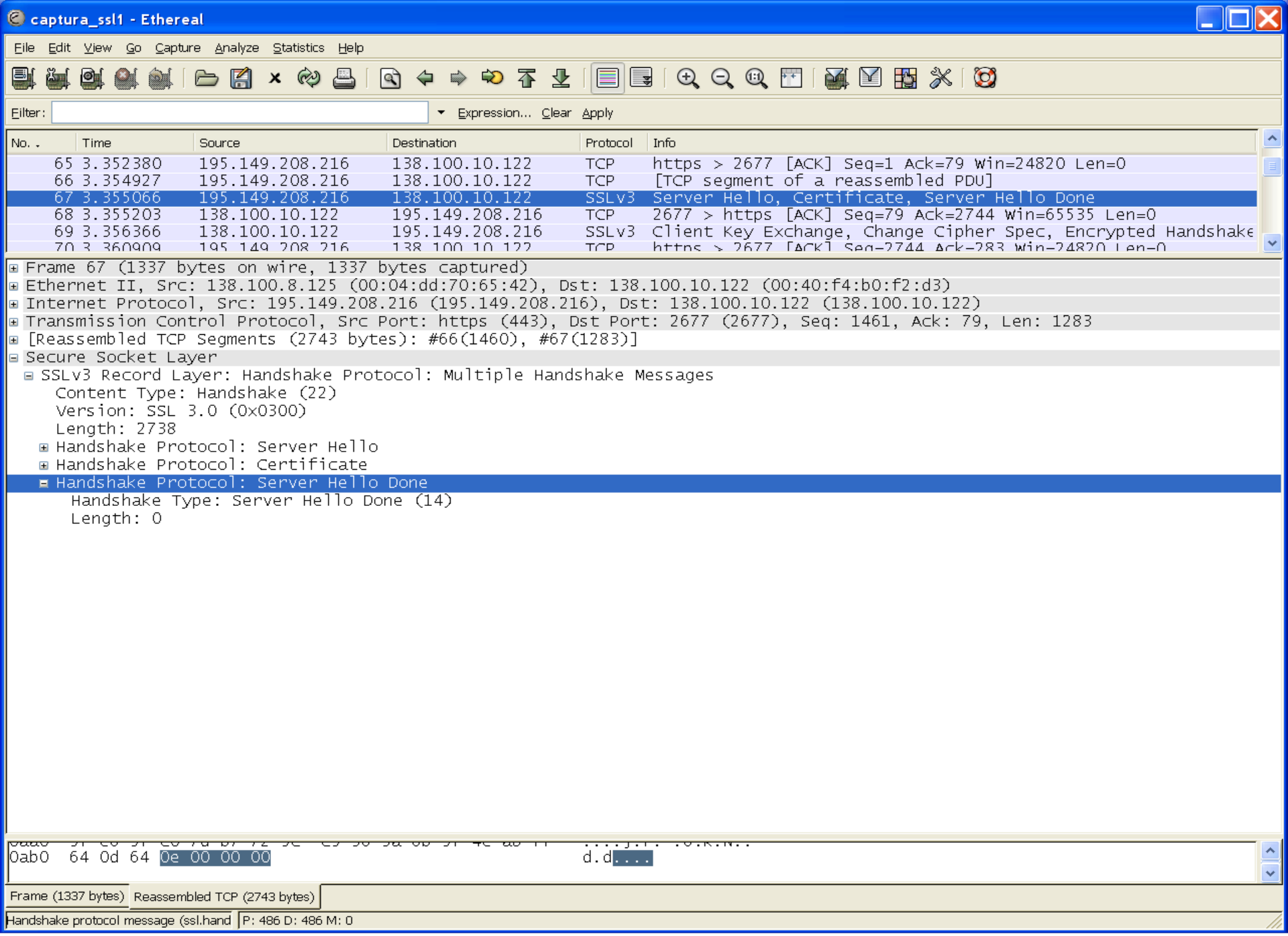

Facultad de Informática - Página Principal - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Stop
Bookmarks Location: http://www.fi.upm.es/
What's Related
Información General
Estudios y Titulaciones
Departamentos y Laboratorios
Servicios
Estudiantes
Noticias
Netscape
Certificate Signers' Certificates
Security Info
Passwords
Navigator
Messenger
Java/JavaScript
Certificates
Yours
People
Web Sites
Signers
Cryptographic Modules
These certificates identify the certificate signers that you accept:
Thawte Personal Premium CA
Thawte Premium Server CA
Thawte Server CA
UPS Document Exchange by DST
Uptime Group Plc. Class 1 CA
Uptime Group Plc. Class 2 CA
Uptime Group Plc. Class 3 CA
Uptime Group Plc. Class 4 CA
VeriSign Class 1 CA - Individual Subscriber - VeriSign, Inc.
VeriSign Class 1 Primary CA
VeriSign Class 2 Primary CA
VeriSign Class 3 Primary CA
VeriSign Class 4 Primary CA
Verisign Class 1 Public Primary Certification Authority - G2
Edit
Verify
Delete
OK
Cancel
Help
m.es
View/Edit...
Inicio Explora... Imengu... Facult... Inbox - ... TEST ... Bookm... RC4 fro... Micros... Faculta... 17:14

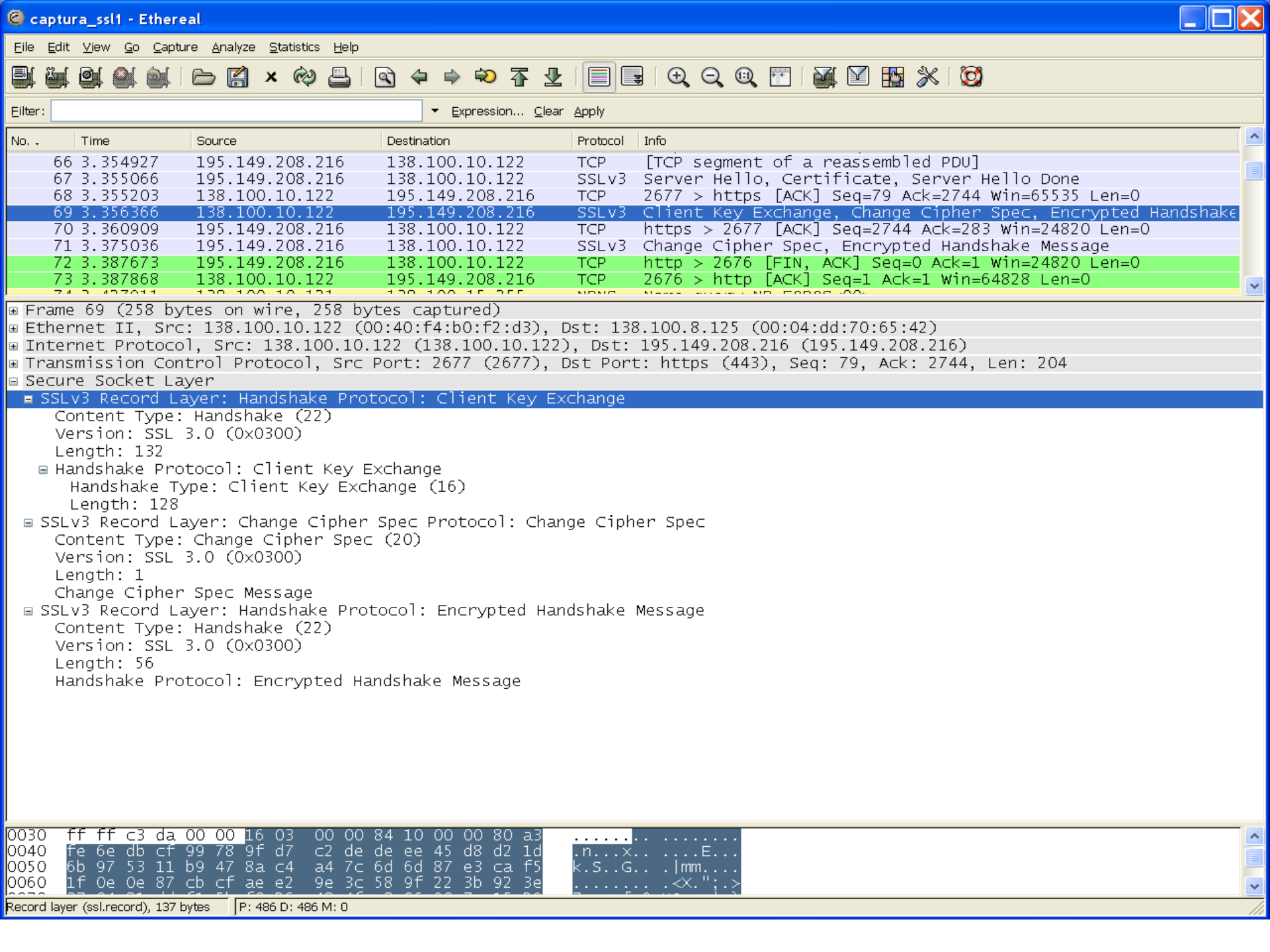

Facultad de Informática - Página Principal - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Stop
Bookmarks Location: http://www.fi.upm.es/
What's Related
Información General
Estudios y Titulaciones
Departamentos y Laboratorios
Servicios
Estudiantes
Noticias
Netscape
Certificate Signers' Certificates
Security Info
These certificates identify the certificate signers that you
Edit A Certification Authority - Netscape
This Certificate belongs to:
Class 1 Public Primary Certification Authority
VeriSign, Inc.
US
This Certificate was issued by:
Class 1 Public Primary Certification Authority
VeriSign, Inc.
US
Serial Number:
00:CD:BA:7F:56:F0:DF:E4:BC:54:FE:22:AC:B3:72:AA:55
This Certificate is valid from Mon Jan 29, 1996 to Wed Aug 02, 2028
Certificate Fingerprint:
97:60:E8:57:5F:D3:50:47:E5:43:0C:94:36:8A:B0:62
This Certificate belongs to a Certifying Authority
Accept this Certificate Authority for Certifying network sites
Accept this Certificate Authority for Certifying e-mail users
Accept this Certificate Authority for Certifying software developers
Warn before sending data to sites certified by this authority
OK
Cancel
Edit
Verify
Delete
OK
Cancel
Help
View/Edit...
Inicio Explora... Imengu... Facult... Inbox - ... TEST ... Bookm... RC4 fro... Micros... Faculta... 17:17

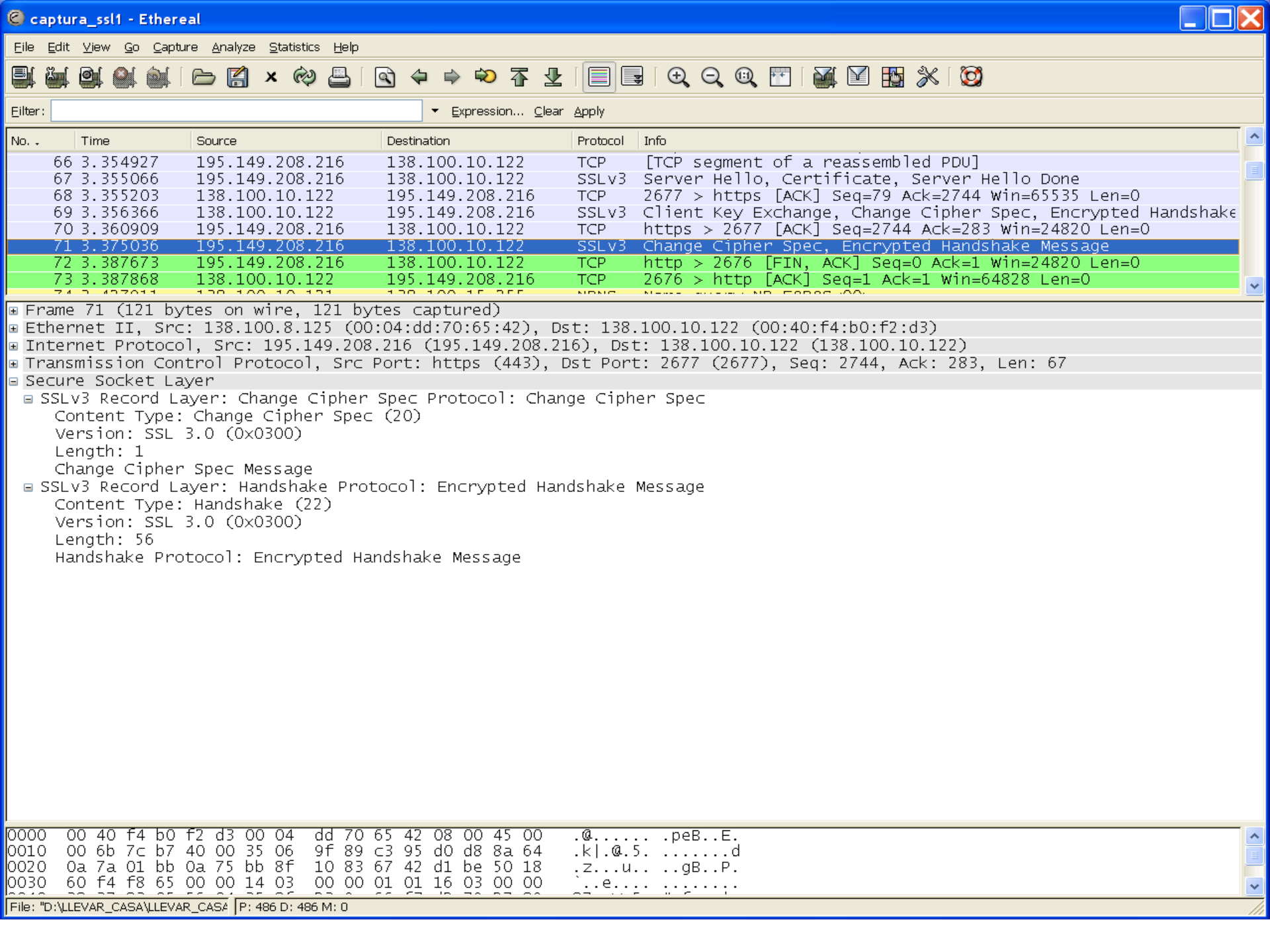

(Untitled) - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
99 3.263782 138.100.10.122 195.149.208.216 TCP 1057 > https [ACK] Seq=1 Ack=1 Win=65535 [TCP CHECKSUM INCORRECT] Len=0
100 3.265920 138.100.10.122 195.149.208.216 SSLv3 Client Hello
101 3.328411 195.149.208.216 138.100.10.122 TCP [TCP ACKed lost segment] http > 1055 [RST] Seq=1 Len=0
Frame 100 (124 bytes on wire, 124 bytes captured)
Ethernet II, Src: AsustekC_8e:78:14 (00:17:31:8e:78:14), Dst: 00:1d:a1:69:34:00 (00:1d:a1:69:34:00)
Internet Protocol, Src: 138.100.10.122 (138.100.10.122), Dst: 195.149.208.216 (195.149.208.216)
Transmission Control Protocol, Src Port: 1057 (1057), Dst Port: https (443), Seq: 1, Ack: 1, Len: 70
Secure Socket Layer
SSLv3 Record Layer: Handshake Protocol: Client Hello
Content Type: Handshake (22)
Version: SSL 3.0 (0x0300)
Length: 65
Handshake Protocol: Client Hello
Handshake Type: Client Hello (1)
Length: 61
Version: SSL 3.0 (0x0300)
Random.gmt_unix_time: Jan 9, 2008 12:33:39.000000000
Random.bytes
Session ID Length: 0
Cipher Suites Length: 22
Cipher Suites (11 suites)
Cipher Suite: TLS_RSA_WITH_RC4_128_MD5 (0x0004)
Cipher Suite: TLS_RSA_WITH_RC4_128_SHA (0x0005)
Cipher Suite: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)
Cipher Suite: TLS_RSA_WITH_DES_CBC_SHA (0x0009)
Cipher Suite: TLS_RSA_EXPORT1024_WITH_RC4_56_SHA (0x0064)
Cipher Suite: TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA (0x0062)
Cipher Suite: TLS_RSA_EXPORT_WITH_RC4_40_MD5 (0x0003)
Cipher Suite: TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 (0x0006)
Cipher Suite: TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA (0x0013)
Cipher Suite: TLS_DHE_DSS_WITH_DES_CBC_SHA (0x0012)
Cipher Suite: TLS_DHE_DSS_EXPORT1024_WITH_DES_CBC_SHA (0x0063)
Compression Methods Length: 1
Compression Methods (1 method)

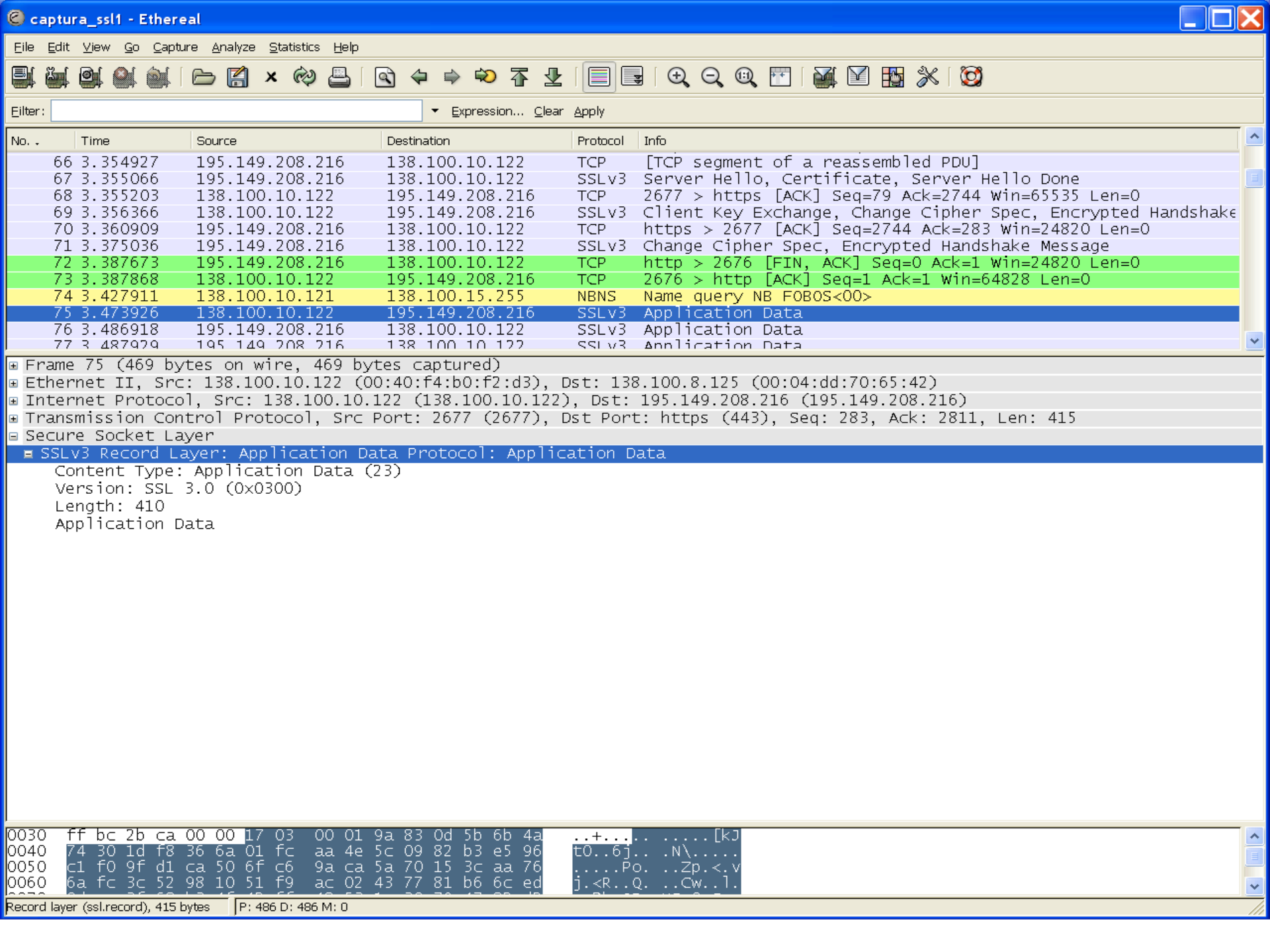

captura_ssl1 - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
65 3.352380 195.149.208.216 138.100.10.122 TCP https > 2677 [ACK] Seq=1 Ack=79 Win=24820 Len=0
66 3.354927 195.149.208.216 138.100.10.122 TCP [TCP segment of a reassembled PDU]
67 3.355066 195.149.208.216 138.100.10.122 SSLv3 Server Hello, Certificate, Server Hello Done
68 3.355203 138.100.10.122 195.149.208.216 TCP 2677 > https [ACK] Seq=79 Ack=2744 Win=65535 Len=0
69 3.356366 138.100.10.122 195.149.208.216 SSLv3 Client Key Exchange, Change Cipher Spec, Encrypted Handshake
Frame 67 (1337 bytes on wire, 1337 bytes captured)
Ethernet II, Src: 138.100.8.125 (00:04:dd:70:65:42), Dst: 138.100.10.122 (00:40:f4:b0:f2:d3)
Internet Protocol, Src: 195.149.208.216 (195.149.208.216), Dst: 138.100.10.122 (138.100.10.122)
Transmission Control Protocol, Src Port: https (443), Dst Port: 2677 (2677), Seq: 1461, Ack: 79, Len: 1283
[Reassembled TCP Segments (2743 bytes): #66(1460), #67(1283)]
Secure Socket Layer
SSLv3 Record Layer: Handshake Protocol: Multiple Handshake Messages
Content Type: Handshake (22)
Version: SSL 3.0 (0x0300)
Length: 2738
Handshake Protocol: Server Hello
Handshake Type: Server Hello (2)
Length: 70
Version: SSL 3.0 (0x0300)
Random.gmt_unix_time: Jan 1, 1970 07:36:58.000000000
Random.bytes
Session ID Length: 32
Session ID (32 bytes)
Cipher Suite: TLS_RSA_WITH_RC4_128_MD5 (0x0004)
Compression Method: null (0)
Handshake Protocol: Certificate
Handshake Protocol: Server Hello Done
0000 16 03 00 0a b2 02 00 00 46 03 00 00 00 5d 0a a3 .... F....]..
0010 82 92 0f 16 f5 ec ad 89 e1 1b 15 75 0c fe 47 c4 ....u..G.
Frame (1337 bytes)
Reassembled TCP (2743 bytes)
Handshake protocol message (ssl.hand
P: 486 D: 486 M: 0

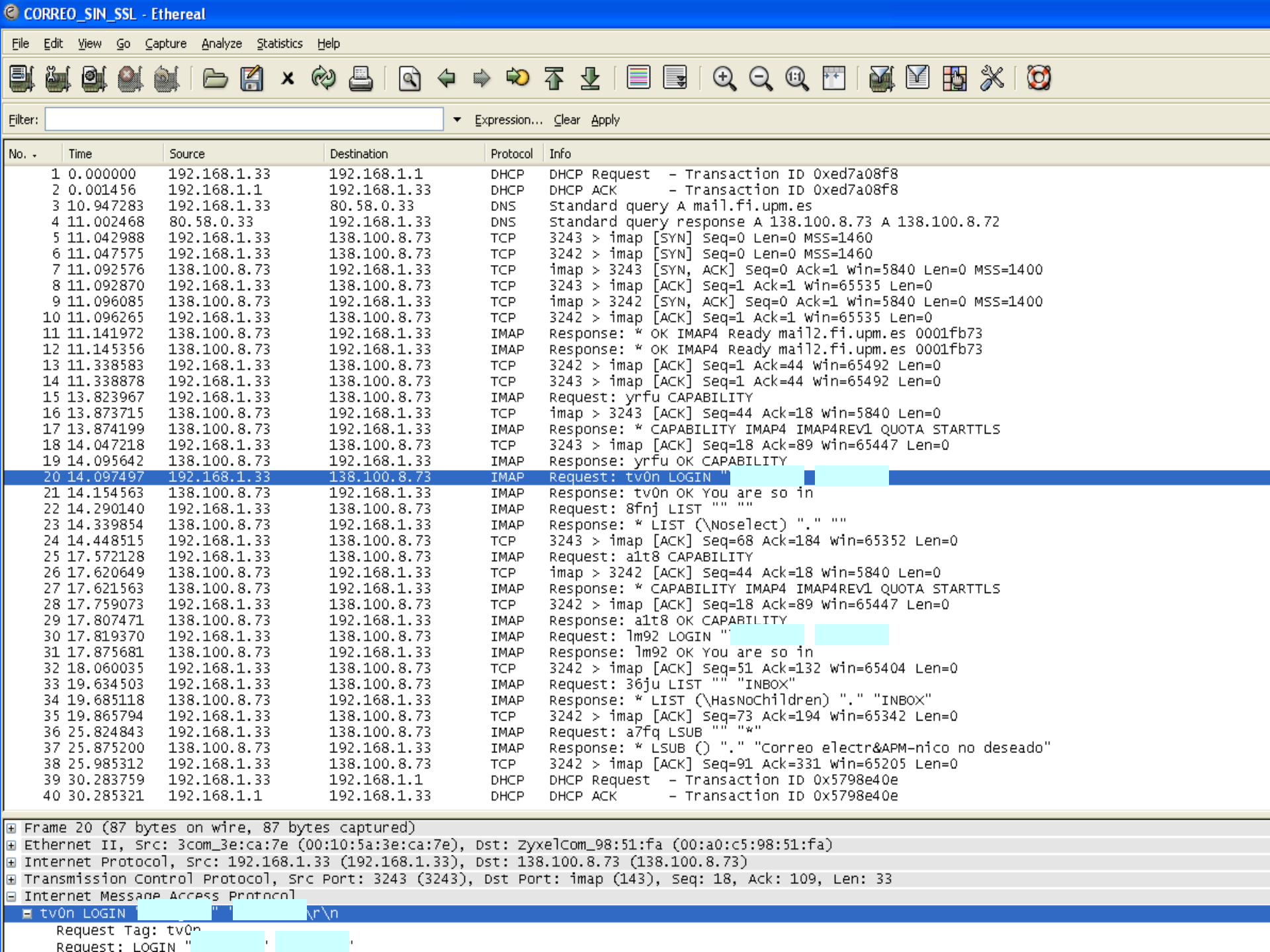

captura_ssl1 - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
65 3.352380 195.149.208.216 138.100.10.122 TCP https > 2677 [ACK] Seq=1 Ack=79 Win=24820 Len=0
66 3.354927 195.149.208.216 138.100.10.122 TCP [TCP segment of a reassembled PDU]
67 3.355066 195.149.208.216 138.100.10.122 SSLv3 Server Hello, Certificate, Server Hello Done
68 3.355203 138.100.10.122 195.149.208.216 TCP 2677 > https [ACK] Seq=79 Ack=2744 Win=65535 Len=0
69 3.356366 138.100.10.122 195.149.208.216 SSLv3 Client Key Exchange, Change Cipher Spec, Encrypted Handshake
Frame 67 (1337 bytes on wire, 1337 bytes captured)
Ethernet II, Src: 138.100.8.125 (00:04:dd:70:65:42), Dst: 138.100.10.122 (00:40:f4:b0:f2:d3)
Internet Protocol, Src: 195.149.208.216 (195.149.208.216), Dst: 138.100.10.122 (138.100.10.122)
Transmission Control Protocol, Src Port: https (443), Dst Port: 2677 (2677), Seq: 1461, Ack: 79, Len: 1283
[Reassembled TCP Segments (2743 bytes): #66(1460), #67(1283)]
Secure Socket Layer
SSLv3 Record Layer: Handshake Protocol: Multiple Handshake Messages
Content Type: Handshake (22)
Version: SSL 3.0 (0x0300)
Length: 2738
Handshake Protocol: Server Hello
Handshake Protocol: Certificate
Handshake Type: Certificate (11)
Length: 2656
Certificates Length: 2653
Certificates (2653 bytes)
Certificate Length: 1165
Certificate: 308203F2A003020102021060 77E043D48DA0D397E56A1FFE...
Certificate Length: 903
Certificate: 308202ECA003020102021025 4B8A853842CCE358F8C5DDAE...
Certificate Length: 576
Certificate: 308201A5021070BAE41D10D92934B638CA7B03CCBABF300D...
signedCertificate
serialNumber : 0x70bae41d10d92934b638ca7b03ccbabf
signature
issuer: rdnSequence (0)
validity
subject: rdnSequence (0)
subjectPublicKeyInfo
algorithmIdentifier
Padding: 0
encrypted: BB4C122BCF2C26004F1413DDA6FBFC0A11848CF3281C6792...
0000 16 03 00 0a b2 02 00 00 46 03 00 00 00 5d 0a a3 ..... F....]..
0010 82 92 0f 16 f5 ec ad 89 e1 1b 15 75 0c fe 47 c4 ....u..G.
Frame (1337 bytes)
Reassembled TCP (2743 bytes)
Record layer version. (ssl.record.versic
P: 486 D: 486 M: 0


captura_ssl1 - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
65 3.352380 195.149.208.216 138.100.10.122 TCP https > 2677 [ACK] Seq=1 Ack=79 Win=24820 Len=0
66 3.354927 195.149.208.216 138.100.10.122 TCP [TCP segment of a reassembled PDU]
67 3.355066 195.149.208.216 138.100.10.122 SSLv3 Server Hello, Certificate, Server Hello Done
68 3.355203 138.100.10.122 195.149.208.216 TCP 2677 > https [ACK] Seq=79 Ack=2744 Win=65535 Len=0
69 3.356366 138.100.10.122 195.149.208.216 SSLv3 Client Key Exchange, Change Cipher Spec, Encrypted Handshake
Frame 67 (1337 bytes on wire, 1337 bytes captured)
Ethernet II, Src: 138.100.8.125 (00:04:dd:70:65:42), Dst: 138.100.10.122 (00:40:f4:b0:f2:d3)
Internet Protocol, Src: 195.149.208.216 (195.149.208.216), Dst: 138.100.10.122 (138.100.10.122)
Transmission Control Protocol, Src Port: https (443), Dst Port: 2677 (2677), Seq: 1461, Ack: 79, Len: 1283
[Reassembled TCP Segments (2743 bytes): #66(1460), #67(1283)]
Secure Socket Layer
SSLv3 Record Layer: Handshake Protocol: Multiple Handshake Messages
Content Type: Handshake (22)
Version: SSL 3.0 (0x0300)
Length: 2738
Handshake Protocol: Server Hello
Handshake Protocol: Certificate
Handshake Protocol: Server Hello Done
Handshake Type: Server Hello Done (14)
Length: 0
0ab0 64 0d 64 0e 00 00 00 d.d....
Frame (1337 bytes)
Reassembled TCP (2743 bytes)
Handshake protocol message (ssl.hand
P: 486 D: 486 M: 0


captura_ssl1 - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
66 3.354927 195.149.208.216 138.100.10.122 TCP [TCP segment of a reassembled PDU]
67 3.355066 195.149.208.216 138.100.10.122 SSLv3 Server Hello, Certificate, Server Hello Done
68 3.355203 138.100.10.122 195.149.208.216 TCP 2677 > https [ACK] Seq=79 Ack=2744 Win=65535 Len=0
69 3.356366 138.100.10.122 195.149.208.216 SSLv3 Client Key Exchange, Change Cipher Spec, Encrypted Handshake
70 3.360909 195.149.208.216 138.100.10.122 TCP https > 2677 [ACK] Seq=2744 Ack=283 Win=24820 Len=0
71 3.375036 195.149.208.216 138.100.10.122 SSLv3 Change Cipher Spec, Encrypted Handshake Message
72 3.387673 195.149.208.216 138.100.10.122 TCP http > 2676 [FIN, ACK] Seq=0 Ack=1 Win=24820 Len=0
73 3.387868 138.100.10.122 195.149.208.216 TCP 2676 > http [ACK] Seq=1 Ack=1 Win=64828 Len=0
Frame 69 (258 bytes on wire, 258 bytes captured)
Ethernet II, Src: 138.100.10.122 (00:40:f4:b0:f2:d3), Dst: 138.100.8.125 (00:04:dd:70:65:42)
Internet Protocol, Src: 138.100.10.122 (138.100.10.122), Dst: 195.149.208.216 (195.149.208.216)
Transmission Control Protocol, Src Port: 2677 (2677), Dst Port: https (443), Seq: 79, Ack: 2744, Len: 204
Secure Socket Layer
SSLv3 Record Layer: Handshake Protocol: Client Key Exchange
Content Type: Handshake (22)
Version: SSL 3.0 (0x0300)
Length: 132
Handshake Protocol: Client Key Exchange
Handshake Type: Client Key Exchange (16)
Length: 128
SSLv3 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
Content Type: Change Cipher Spec (20)
Version: SSL 3.0 (0x0300)
Length: 1
Change Cipher Spec Message
SSLv3 Record Layer: Handshake Protocol: Encrypted Handshake Message
Content Type: Handshake (22)
Version: SSL 3.0 (0x0300)
Length: 56
Handshake Protocol: Encrypted Handshake Message
0030 ff ff c3 da 00 00 16 03 00 00 84 10 00 00 80 a3
0040 fe 6e db cf 99 78 9f d7 c2 de de ee 45 d8 d2 1d
0050 6b 97 53 11 b9 47 8a c4 a4 7c 6d 6d 87 e3 ca f5
0060 1f 0e 0e 87 cb cf ae e2 9e 3c 58 9f 22 3b 92 3e
Record layer (ssl.record), 137 bytes
P: 486 D: 486 M: 0


captura_ssl1 - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
66 3.354927 195.149.208.216 138.100.10.122 TCP [TCP segment of a reassembled PDU]
67 3.355066 195.149.208.216 138.100.10.122 SSLv3 Server Hello, Certificate, Server Hello Done
68 3.355203 138.100.10.122 195.149.208.216 TCP 2677 > https [ACK] Seq=79 Ack=2744 Win=65535 Len=0
69 3.356366 138.100.10.122 195.149.208.216 SSLv3 Client Key Exchange, Change Cipher Spec, Encrypted Handshake
70 3.360909 195.149.208.216 138.100.10.122 TCP https > 2677 [ACK] Seq=2744 Ack=283 Win=24820 Len=0
71 3.375036 195.149.208.216 138.100.10.122 SSLv3 Change Cipher Spec, Encrypted Handshake Message
72 3.387673 195.149.208.216 138.100.10.122 TCP http > 2676 [FIN, ACK] Seq=0 Ack=1 Win=24820 Len=0
73 3.387868 138.100.10.122 195.149.208.216 TCP 2676 > http [ACK] Seq=1 Ack=1 Win=64828 Len=0
Frame 71 (121 bytes on wire, 121 bytes captured)
Ethernet II, Src: 138.100.8.125 (00:04:dd:70:65:42), Dst: 138.100.10.122 (00:40:f4:b0:f2:d3)
Internet Protocol, Src: 195.149.208.216 (195.149.208.216), Dst: 138.100.10.122 (138.100.10.122)
Transmission Control Protocol, Src Port: https (443), Dst Port: 2677 (2677), Seq: 2744, Ack: 283, Len: 67
Secure Socket Layer
SSLv3 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
Content Type: Change Cipher Spec (20)
Version: SSL 3.0 (0x0300)
Length: 1
Change Cipher Spec Message
SSLv3 Record Layer: Handshake Protocol: Encrypted Handshake Message
Content Type: Handshake (22)
Version: SSL 3.0 (0x0300)
Length: 56
Handshake Protocol: Encrypted Handshake Message
0000 00 40 f4 b0 f2 d3 00 04 dd 70 65 42 08 00 45 00 .@..... .peB..E.
0010 00 6b 7c b7 40 00 35 06 9f 89 c3 95 d0 d8 8a 64 .k|.@.5. ....d
0020 0a 7a 01 bb 0a 75 bb 8f 10 83 67 42 d1 be 50 18 .z...u.. ..gB..P.
0030 60 f4 f8 65 00 00 14 03 00 00 01 01 16 03 00 00 `..e.... ....
File: "D:\LLEVAR_CASA\LLEVAR_CASA P: 486 D: 486 M: 0

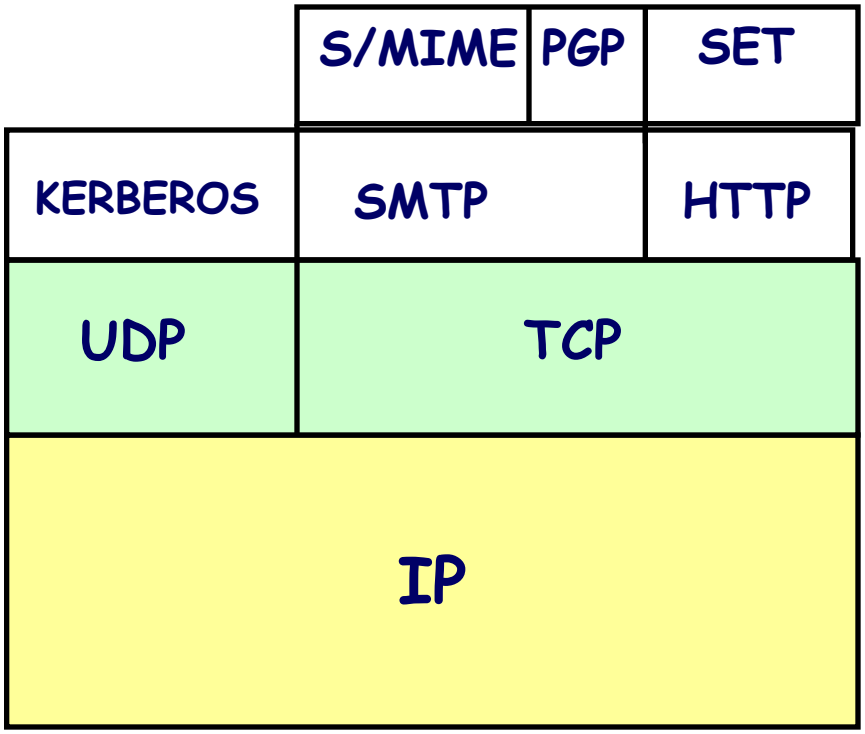

captura_ssl1 - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
66 3.354927 195.149.208.216 138.100.10.122 TCP [TCP segment of a reassembled PDU]
67 3.355066 195.149.208.216 138.100.10.122 SSLv3 Server Hello, Certificate, Server Hello Done
68 3.355203 138.100.10.122 195.149.208.216 TCP 2677 > https [ACK] Seq=79 Ack=2744 Win=65535 Len=0
69 3.356366 138.100.10.122 195.149.208.216 SSLv3 Client Key Exchange, Change Cipher Spec, Encrypted Handshake
70 3.360909 195.149.208.216 138.100.10.122 TCP https > 2677 [ACK] Seq=2744 Ack=283 Win=24820 Len=0
71 3.375036 195.149.208.216 138.100.10.122 SSLv3 Change Cipher Spec, Encrypted Handshake Message
72 3.387673 195.149.208.216 138.100.10.122 TCP http > 2676 [FIN, ACK] Seq=0 Ack=1 Win=24820 Len=0
73 3.387868 138.100.10.122 195.149.208.216 TCP 2676 > http [ACK] Seq=1 Ack=1 Win=64828 Len=0
74 3.427911 138.100.10.121 138.100.15.255 NBNS Name query NB FOBOS<00>
75 3.473926 138.100.10.122 195.149.208.216 SSLv3 Application Data
76 3.486918 195.149.208.216 138.100.10.122 SSLv3 Application Data
Frame 75 (469 bytes on wire, 469 bytes captured)
Ethernet II, Src: 138.100.10.122 (00:40:f4:b0:f2:d3), Dst: 138.100.8.125 (00:04:dd:70:65:42)
Internet Protocol, Src: 138.100.10.122 (138.100.10.122), Dst: 195.149.208.216 (195.149.208.216)
Transmission Control Protocol, Src Port: 2677 (2677), Dst Port: https (443), Seq: 283, Ack: 2811, Len: 415
Secure Socket Layer
SSLv3 Record Layer: Application Data Protocol: Application Data
Content Type: Application Data (23)
Version: SSL 3.0 (0x0300)
Length: 410
Application Data
0030 ff bc 2b ca 00 00 17 03 00 01 9a 83 0d 5b 6b 4a ..+.. ....[kJ
0040 74 30 1d f8 36 6a 01 fc aa 4e 5c 09 82 b3 e5 96 t0..6j.. .N\.....
0050 c1 f0 9f d1 ca 50 6f c6 9a ca 5a 70 15 3c aa 76 .....Po. ..Zp.<.v
0060 6a fc 3c 52 98 10 51 f9 ac 02 43 77 81 b6 6c ed j.<R..Q. ..Cw..l.
Record layer (ssl.record), 415 bytes
P: 486 D: 486 M: 0


CORREO_SIN_SSL - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
1 0.000000 192.168.1.33 192.168.1.1 DHCP DHCP Request - Transaction ID 0xed7a08f8
2 0.001456 192.168.1.1 192.168.1.33 DHCP DHCP ACK - Transaction ID 0xed7a08f8
3 10.947283 192.168.1.33 80.58.0.33 DNS Standard query A mail.fi.upm.es
4 11.002468 80.58.0.33 192.168.1.33 DNS Standard query response A 138.100.8.73 A 138.100.8.72
5 11.042988 192.168.1.33 138.100.8.73 TCP 3243 > imap [SYN] Seq=0 Len=0 MSS=1460
6 11.047575 192.168.1.33 138.100.8.73 TCP 3242 > imap [SYN] Seq=0 Len=0 MSS=1460
7 11.092576 138.100.8.73 192.168.1.33 TCP imap > 3243 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1400
8 11.092870 192.168.1.33 138.100.8.73 TCP 3243 > imap [ACK] Seq=1 Ack=1 Win=65535 Len=0
9 11.096085 138.100.8.73 192.168.1.33 TCP imap > 3242 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1400
10 11.096265 192.168.1.33 138.100.8.73 TCP 3242 > imap [ACK] Seq=1 Ack=1 Win=65535 Len=0
11 11.141972 138.100.8.73 192.168.1.33 IMAP Response: * OK IMAP4 Ready mail2.fi.upm.es 0001fb73
12 11.145356 138.100.8.73 192.168.1.33 IMAP Response: * OK IMAP4 Ready mail2.fi.upm.es 0001fb73
13 11.338583 192.168.1.33 138.100.8.73 TCP 3242 > imap [ACK] Seq=1 Ack=44 Win=65492 Len=0
14 11.338878 192.168.1.33 138.100.8.73 TCP 3243 > imap [ACK] Seq=1 Ack=44 Win=65492 Len=0
15 13.823967 192.168.1.33 138.100.8.73 IMAP Request: yrfu CAPABILITY
16 13.873715 138.100.8.73 192.168.1.33 TCP imap > 3243 [ACK] Seq=44 Ack=18 Win=5840 Len=0
17 13.874199 138.100.8.73 192.168.1.33 IMAP Response: * CAPABILITY IMAP4 IMAP4REV1 QUOTA STARTTLS
18 14.047218 192.168.1.33 138.100.8.73 TCP 3243 > imap [ACK] Seq=18 Ack=89 Win=65447 Len=0
19 14.095642 138.100.8.73 192.168.1.33 IMAP Response: yrfu OK CAPABILITY
20 14.097497 192.168.1.33 138.100.8.73 IMAP Request: tv0n LOGIN "
21 14.154563 138.100.8.73 192.168.1.33 IMAP Response: tv0n OK You are so in
22 14.290140 192.168.1.33 138.100.8.73 IMAP Request: 8fnj LIST "" ""
23 14.339854 138.100.8.73 192.168.1.33 IMAP Response: * LIST (\Noselect) "." ""
24 14.448515 192.168.1.33 138.100.8.73 TCP 3243 > imap [ACK] Seq=68 Ack=184 Win=65352 Len=0
25 17.572128 192.168.1.33 138.100.8.73 IMAP Request: a1t8 CAPABILITY
26 17.620649 138.100.8.73 192.168.1.33 TCP imap > 3242 [ACK] Seq=44 Ack=18 Win=5840 Len=0
27 17.621563 138.100.8.73 192.168.1.33 IMAP Response: * CAPABILITY IMAP4 IMAP4REV1 QUOTA STARTTLS
28 17.759073 192.168.1.33 138.100.8.73 TCP 3242 > imap [ACK] Seq=18 Ack=89 Win=65447 Len=0
29 17.807471 138.100.8.73 192.168.1.33 IMAP Response: a1t8 OK CAPABILITY
30 17.819370 192.168.1.33 138.100.8.73 IMAP Request: lm92 LOGIN "
31 17.875681 138.100.8.73 192.168.1.33 IMAP Response: lm92 OK You are so in
32 18.060035 192.168.1.33 138.100.8.73 TCP 3242 > imap [ACK] Seq=51 Ack=132 Win=65404 Len=0
33 19.634503 192.168.1.33 138.100.8.73 IMAP Request: 36ju LIST "" "INBOX"
34 19.685118 138.100.8.73 192.168.1.33 IMAP Response: * LIST (\HasNoChildren) "." "INBOX"
35 19.865794 192.168.1.33 138.100.8.73 TCP 3242 > imap [ACK] Seq=73 Ack=194 Win=65342 Len=0
36 25.824843 192.168.1.33 138.100.8.73 IMAP Request: a7fq LSUB "" "*"
37 25.875200 138.100.8.73 192.168.1.33 IMAP Response: * LSUB () "." "Correo electr&APM-nico no deseado"
38 25.985312 192.168.1.33 138.100.8.73 TCP 3242 > imap [ACK] Seq=91 Ack=331 Win=65205 Len=0
39 30.283759 192.168.1.33 192.168.1.1 DHCP DHCP Request - Transaction ID 0x5798e40e
40 30.285321 192.168.1.1 192.168.1.33 DHCP DHCP ACK - Transaction ID 0x5798e40e
Frame 20 (87 bytes on wire, 87 bytes captured)
Ethernet II, Src: 3com_3e:ca:7e (00:10:5a:3e:ca:7e), Dst: ZyxelCom_98:51:fa (00:a0:c5:98:51:fa)
Internet Protocol, Src: 192.168.1.33 (192.168.1.33), Dst: 138.100.8.73 (138.100.8.73)
Transmission Control Protocol, Src Port: 3243 (3243), Dst Port: imap (143), Seq: 18, Ack: 109, Len: 33
Internet Message Access Protocol
tv0n LOGIN " "\r\n
Request Tag: tv0n
Request: LOGIN "

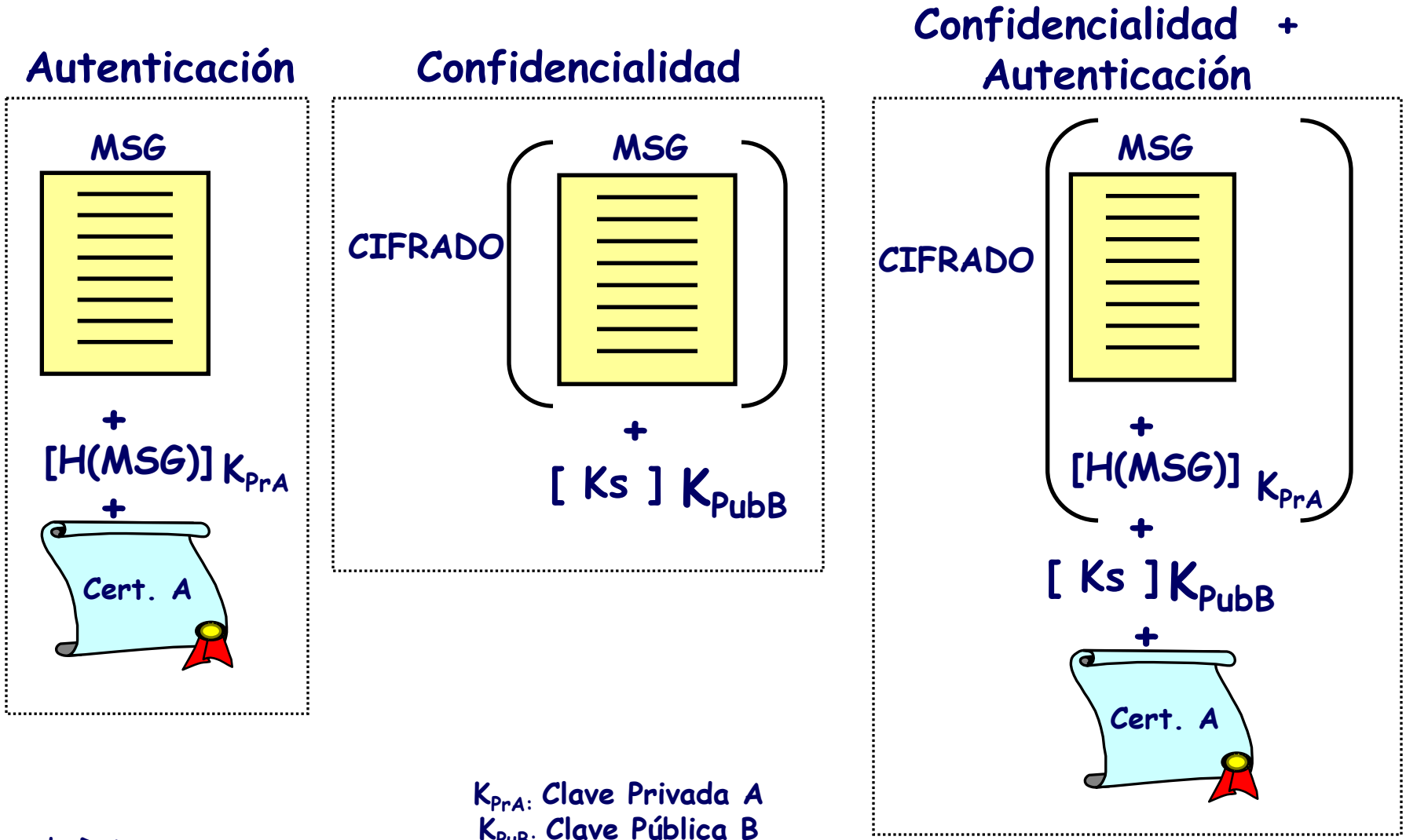
TLS (Transport Layer Security)

- Estándar RFC 2246 basado en SSLv3
- No puede interoperar con SSLv3
  - Diferente forma de obtener la Premaster Key
  - El mensaje Certificate_verify se calcula de forma diferente

SEGURIDAD EN EL NIVEL DE APLICACIÓN



Servicios de Seguridad
Correo Electrónico



K_{PrA}: Clave Privada A
K_{PuB}: Clave Pública B

CORREO ELECTRÓNICO SEGURO

- S/MIME (Secure Multipurpose Internet Mail Extensions)
  - Estándar de Internet
  - RFC 2632 …2643
  - Usa certificados X.509
- (PGP) Pretty Good Privacy
  - Diseñado por P. Zimmermann (1995)
  - Estándar de hecho para ordenadores personales
  - Código abierto. Varias versiones